

Hitachi Data Ingestor

6.4.5-01

Single Node Administrator's Guide

This manual explains how to operate a Hitachi Data Ingestor (HDI) in a single-node configuration.

© 2017- 2018 Hitachi Vantara Corporation. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying 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 to access relevant data; and
- 2) Verifying that 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.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

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, RS6000, 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.

InterScan is a trademark of Trend Micro Incorporated.

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



Contents

Preface.....	xiii
Intended audience.....	xiv
Product version.....	xiv
Release notes.....	xiv
Organization of HDI manuals.....	xiv
Abbreviation conventions.....	xv
Document conventions.....	xvi
Convention for storage capacity values.....	xvi
Accessing product documentation.....	xvii
Getting help.....	xvii
Comments.....	xvii
1 Logging on.....	1-1
Logging on to the system.....	1-2
2 Managing system administrator accounts.....	2-1
Changing an account password.....	2-2
Changing account security settings.....	2-2
3 Managing shared directories.....	3-1
Creating a shared directory.....	3-2
Referencing other HDI data as read-only via the linked HCP.....	3-3
Changing the policy and schedule for migrating data to HCP.....	3-4
Setting conditions for preventing certain files from turning into stub files.....	3-5
Expanding the capacity of a file system.....	3-6
Importing data from another file server.....	3-6
Importing data from another file server by using the CIFS protocol.....	3-7
Importing data from another file server by using the NFS protocol.....	3-11
4 Setting up the access environment from clients.....	4-1
Setting up the access environment from CIFS clients.....	4-2
Joining a node to an Active Directory domain.....	4-2
Rejoining an Active Directory domain.....	4-5
Joining a node to an NT domain.....	4-5

Configuring a workgroup.....	4-7
Identifying users by user mapping.....	4-9
Collecting CIFS client access logs.....	4-10
Setting up the access environment from NFS clients.....	4-11
5 Showing previous data.....	5-1
Showing previous data on HCP.....	5-2
6 Managing disk capacity.....	6-1
Increasing the number of disks.....	6-2
Adding internal hard disks to a node.....	6-2
Adding LUs to a running storage system.....	6-3
Changing the use of disks.....	6-4
Deleting a volume group.....	6-4
Deleting LUs that are not being used by file systems from a volume group.....	6-4
7 Protecting user data.....	7-1
Setting up virus scanning.....	7-2
Backing up data to a tape device.....	7-2
Restoring data from a tape device.....	7-4
8 Backing up system configuration.....	8-1
Manually backing up the system configuration.....	8-2
Regularly backing up system configuration.....	8-2
9 Changing the network configuration.....	9-1
Changing the IP address of a node.....	9-2
Changing the host name of a node.....	9-3
Adding and deleting routing information.....	9-4
Adding routing information.....	9-4
Deleting routing information.....	9-4
Changing the negotiation mode.....	9-5
Changing the negotiation mode (for a non-cascaded trunk port).....	9-5
Changing the negotiation mode (for a cascaded trunk port).....	9-6
Setting up redundant link configuration.....	9-7
Setting link aggregation.....	9-7
Setting link alternation.....	9-8
Combining link aggregation and link alternation (cascaded trunking).....	9-9
Performing manual link alternation.....	9-10
Setting up a VLAN.....	9-10
10 Monitoring the system.....	10-1
Using SNMP.....	10-2
Using SNMPv2 in an IPv4 environment.....	10-2
Using SNMPv2 in an IPv6 environment or SNMPv3.....	10-3
Using error email notifications.....	10-6

11	Setting up an environment for command and GUI operations.....	11-1
	Setting up the SSH environment to use commands.....	11-2
	Setting up a public key certificate.....	11-2
12	Performing an update installation.....	12-1
	Updating software.....	12-2
	Updating software (using the installation file registered in an HCP system).....	12-2
	Updating software (using an installation media).....	12-3
A	Operations provided by the GUI.....	A-1
	List of operations.....	A-2
B	Basic GUI operation.....	B-1
	Window configuration.....	B-2
	Notes on using the GUI.....	B-5
C	GUI reference.....	C-1
	Migration Tasks dialog box.....	C-4
	migration-task page.....	C-7
	Task Information tab.....	C-8
	History tab.....	C-11
	Download Report dialog box.....	C-12
	Failed dialog box.....	C-12
	Policy Information dialog box.....	C-13
	Migration Task Wizard.....	C-15
	2. Task Settings page.....	C-17
	3. Schedule Settings page.....	C-17
	4. Policy Settings page.....	C-18
	File Systems dialog box.....	C-19
	Stop Task dialog box.....	C-20
	Migrate Immediately dialog box.....	C-20
	Enable Task dialog box.....	C-21
	Disable Task dialog box.....	C-21
	Delete Task dialog box.....	C-22
	System Configuration Wizard.....	C-23
	Service Configuration Wizard.....	C-24
	Download Chargeback Report dialog box.....	C-26
	Import Files dialog box.....	C-27
	Configure Proxy Server dialog box.....	C-34
	Change System Admin Password dialog box.....	C-35
	Change HCP Tenant Admin Password dialog box.....	C-36
	Update HCP Anywhere Credentials dialog box.....	C-37
	Login Security dialog box.....	C-38
	Check for Errors dialog box.....	C-39
	List of RAS Information page.....	C-39
	List of RAS Information page (for List of messages).....	C-40
	List of RAS Information page (for List of system logs).....	C-41
	List of RAS Information page (for List of other log files).....	C-42
	List of RAS Information page (for Batch-download).....	C-42

List of RAS Information page (for List of core files).....	C-43
List of RAS Information page (for Server check).....	C-44
Transfer All Files page.....	C-45
Dashboard tab.....	C-45
System Information panel.....	C-46
Capacity Usage panel.....	C-47
Namespace Information panel.....	C-48
Tasks panel.....	C-49
Panel Configuration dialog box.....	C-50
host-name window.....	C-51
Shares window.....	C-53
File Systems window.....	C-56
File Systems tab.....	C-57
Cache Resident tab.....	C-60
file-system-name window.....	C-61
Monitor tab.....	C-62
Shares tab.....	C-63
Namespace tab.....	C-65
Properties tab.....	C-67
Cache Resident Policy tab.....	C-69
Volume Groups window.....	C-70
Hardware window.....	C-72
Hardware tab.....	C-75
Network tab.....	C-77
Memory tab.....	C-79
tenant-name window.....	C-79
Namespaces tab.....	C-80
Properties tab.....	C-81
Import Files window.....	C-81
Restart Node dialog box.....	C-84
System Software Installation dialog box.....	C-85
Local Users dialog box.....	C-85
List of Users / Groups page.....	C-85
Change Password page.....	C-87
Edit User page.....	C-87
Add User page.....	C-88
Batch Operation page.....	C-89
CSV file format.....	C-90
Execution results file format.....	C-92
Edit Group page.....	C-95
Add Group page.....	C-96
Backup Configuration dialog box.....	C-97
Save System Settings Menu page.....	C-98
Save All System Settings page.....	C-98
Schedule Settings for Saving All System Settings page.....	C-100
List of Mounted File Systems page.....	C-102
Upload Saved Data page.....	C-102
Network & System Configuration dialog box.....	C-103
System Setup Menu page.....	C-103
List of Data Ports page.....	C-105
Negotiation Mode Setup page.....	C-107
List of Trunking Configurations page.....	C-111

Link Aggregation Setup page.....	C-113
Link Alternation Setup page.....	C-114
List of Interfaces page.....	C-114
Edit Interface page.....	C-115
Add Interface page.....	C-116
DNS, NIS, LDAP Setup page.....	C-117
List of Routings page.....	C-119
Add Routing page.....	C-120
Time Setup page.....	C-122
Syslog Setup page.....	C-123
Edit Syslog Setup page.....	C-124
Add Syslog Setup page.....	C-124
Log File Capacity Setup page.....	C-125
Edit File Capacity page.....	C-125
Core File Auto. Deletion Setup page.....	C-126
Edit System File page.....	C-126
Performance Tuning page.....	C-133
List of SNMPs page.....	C-134
Edit SNMP page.....	C-135
Add SNMP page.....	C-136
Access Protocol Configuration dialog box.....	C-137
List of Services page.....	C-137
CIFS Service Management (Basic) page.....	C-141
CIFS Service Management (User mapping) page.....	C-143
CIFS Service Management (Security) page.....	C-149
CIFS Service Management (Performance) page.....	C-153
CIFS Service Management (Administration) page.....	C-156
Select Authentication Mode page.....	C-157
Local Authentication page.....	C-158
NT Domain Authentication page.....	C-158
Active Directory Authentication page.....	C-159
Setting Events Logged to the CIFS Access Log page.....	C-161
FTP Service Management page.....	C-162
List of Mounted File Systems page.....	C-166
Select FTP Users page.....	C-167
NFS Service Management page.....	C-168
SFTP Service Management page.....	C-171
Select SFTP Users page.....	C-175
Public Key List page.....	C-176
Add Public Key page.....	C-176
CIFS Service Maintenance page.....	C-177
Virus Scan Server Configuration dialog box.....	C-186
List of Scanner Servers page.....	C-186
Edit Scanner Server page.....	C-189
Add Scanner Server page.....	C-189
Scan Conditions page.....	C-190
Scanning software page.....	C-196
CIFS Protocol Settings dialog box.....	C-197
NFS Protocol Settings dialog box.....	C-198
Edit Share dialog box.....	C-198
Release Share(s) dialog box.....	C-204
Edit CIFS Share Host or Network dialog box.....	C-204

Add CIFS Share Host or Network dialog box.....	C-205
Edit NFS Share Host or Network dialog box.....	C-206
Add NFS Share Host or Network dialog box.....	C-207
Add Share dialog box.....	C-208
Create File System dialog box.....	C-215
Edit File System dialog box.....	C-228
Delete File System dialog box.....	C-235
Advanced ACL Settings dialog box.....	C-235
Add Cache Resident Policy dialog box.....	C-237
Edit Cache Resident Policy dialog box.....	C-237
Delete Cache Resident Policy dialog box.....	C-238
Provisioning Wizard.....	C-238
D Operation performed by end users.....	D-1
List of operations.....	D-2
Logging on.....	D-2
Basic GUI operations.....	D-2
GUI layout.....	D-2
Notes about using the GUI.....	D-3
GUI reference.....	D-3
List of File Shares page (for List of NFS file shares).....	D-3
List of File Shares page (for List of CIFS File Shares).....	D-4
Display Quota page (for User Quota Info.).....	D-4
Display Quota page (for Group Quota Info.).....	D-6
Password Setup page.....	D-8
User Info. Setup page.....	D-8
E Reserved words.....	E-1
List of reserved words.....	E-2
F MIB objects.....	F-1
List of MIB objects.....	F-2
MIB objects for responding to SNMP get requests.....	F-3
The typical MIB objects.....	F-3
List of MIB object.....	F-5
MIB objects used for SNMP traps.....	F-68
G Operation reference information.....	G-1
List of reference information.....	G-2
H Node maintenance.....	H-1
Starting and forcibly stopping a node OS.....	H-2
Starting an OS.....	H-2
Forcibly Stopping an OS.....	H-2
Replacing the internal RAID battery.....	H-2
Managing the RAID card.....	H-3

I Terminology used in messages and related documents.....	I-1
Viewing messages and related documents.....	I-2
J Acronyms.....	J-1
Acronyms used in the HDI manuals.....	J-2

Glossary

Index



Preface

This manual explains how to operate a Hitachi Data Ingestor (HDI) in a single-node configuration.

This preface includes the following information:

- [Intended audience](#)
- [Product version](#)
- [Release notes](#)
- [Organization of HDI manuals](#)
- [Abbreviation conventions](#)
- [Document conventions](#)
- [Convention for storage capacity values](#)
- [Accessing product documentation](#)
- [Getting help](#)
- [Comments](#)

Intended audience

This manual is intended for system administrators who operate and manage HDI systems in a single-node configuration.

Also, the user must have:

- A basic knowledge of Hitachi Content Platform (HCP) systems
- A basic knowledge of networks
- A basic knowledge of file sharing services
- A basic knowledge of CIFS
- A basic knowledge of NFS
- A basic knowledge of Windows
- A basic knowledge of Web browsers

Product version

This document revision applies to Hitachi Data Ingestor version 4.2.1 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>.

Organization of HDI manuals

HDI manuals are organized as shown below.

Note that whether HDI nodes can be set up in a redundant configuration depends on the HDI model. A configuration where nodes are made redundant is called a cluster configuration, and a configuration where a node is not made redundant with another node is called a single-node configuration. Which manuals you need to read depends on which configuration you are going to use.

Manual name	Description
<i>Hitachi Data Ingestor Installation and Configuration Guide</i> , MK-90HDICOM002	You must read this manual first to use an HDI system. This manual contains the information that you must be aware of before starting HDI system operation, as well as the environment settings for an external server.
<i>Hitachi Data Ingestor Cluster Getting Started Guide</i> , MK-90HDICOM001	This manual explains how to set up an HDI system in a cluster configuration.

Manual name	Description
<i>Hitachi Data Ingestor Cluster Administrator's Guide, MK-90HDI038</i>	This manual provides procedures for using HDI systems in a cluster configuration, as well as provides GUI references.
<i>Hitachi Data Ingestor Cluster Troubleshooting Guide, MK-90HDI029</i>	This manual provides troubleshooting information for HDI systems in a cluster configuration.
<i>Hitachi Data Ingestor Single Node Getting Started Guide, MK-90HDI028</i>	This manual explains how to set up an HDI system in a single-node configuration.
<i>Hitachi Data Ingestor Single Node Administrator's Guide (This manual)</i>	This manual explains the procedures for using HDI systems in a single-node configuration, as well as provides GUI references.
<i>Hitachi Data Ingestor Single Node Troubleshooting Guide, MK-90HDI030</i>	This manual provides troubleshooting information for HDI systems in a single-node configuration.
<i>Hitachi Data Ingestor CLI Administrator's Guide, MK-90HDI034</i>	This manual describes the syntax of the commands that can be used for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor API References, MK-90HDI026</i>	This manual explains how to use the API for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor Error Codes, MK-90HDI005</i>	This manual contains messages for HDI systems in a cluster configuration or a single-node configuration.
<i>Hitachi Data Ingestor File System Protocols (CIFS/NFS) Administrator's Guide, MK-90HDI035</i>	This manual contains the things to keep in mind before using the CIFS or NFS service of an HDI system in a cluster configuration or a single-node configuration from a CIFS or NFS client.

The *Cluster Administrator's Guide* and the *Single Node Administrator's Guide* are available in HTML and PDF formats. All other manuals are available in only PDF format.

Abbreviation conventions

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
Active Directory	Active Directory(R)
Dynamic Provisioning	Hitachi Dynamic Provisioning
Dynamic Tiering	Hitachi Dynamic Tiering
HCP	Hitachi Content Platform
HDI	Hitachi Data Ingestor
Internet Explorer	Windows(R) Internet Explorer(R)



Abbreviation	Full name or meaning
Windows	Microsoft(R) Windows(R) Operating System

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click OK .
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: <i>copy source-file target-file</i> Note: Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user. Example: # pairdisplay -g oradb
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: # pairdisplay -g <group> Note: Italic font is also used to indicate variables.
[] square brackets	Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing.

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

Icon	Label	Description
	Note	Calls attention to important and/or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.

Convention for storage capacity values

Storage capacity values (e.g., drive capacity) are calculated based on the following values:

Capacity Unit	Physical Value	Logical Value
1 KB	1,000 bytes	1,024 (2^{10}) bytes
1 MB	1,000 KB or 1,000 ² bytes	1,024 KB or 1,024 ² bytes

Capacity Unit	Physical Value	Logical Value
1 GB	1,000 MB or 1,000 ³ bytes	1,024 MB or 1,024 ³ bytes
1 TB	1,000 GB or 1,000 ⁴ bytes	1,024 GB or 1,024 ⁴ bytes
1 PB	1,000 TB or 1,000 ⁵ bytes	1,024 TB or 1,024 ⁵ bytes
1 EB	1,000 PB or 1,000 ⁶ bytes	1,024 PB or 1,024 ⁶ bytes
1 block	-	512 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!

Logging on

This chapter describes how to log on the system.

- [Logging on to the system](#)

Logging on to the system

A system administrator can operate and manage a Hitachi Data Ingestor (HDI) system from a Web browser by logging on to the system.

To log on to the system

1. If you are using UPnP, click the HDI icon in **Other Devices**, which appears in the network list in the management console.
If you are not using UPnP, enter the URL in your web browser's address bar, in the following format:
`https://HDI-IP-address-or-host-name/admin/`
The Login window appears.
2. Specify a user ID and the password in the Login window, and then click **Login**.
The main window is displayed.



Note:

- If you are accessing the GUI for the first time, use the following account to log on.
User ID: `admin`
Password: `chang3me!` (default)
When you access the GUI for the first time, the **Change System Admin Password** dialog box is displayed ([Change System Admin Password dialog box on page C-35](#)). Be sure to change the password to prevent unpermitted access.
 - The user ID and password here are shared with the HDI API administrator account. If the password is changed from the API, use the new password.
-

Managing system administrator accounts

This chapter describes how to manage system administrator accounts.

- [Changing an account password](#)
- [Changing account security settings](#)

Changing an account password

A system administrator can change his or her own password.

GUI used for this operation

- [Change System Admin Password dialog box on page C-35](#)

To change an account password

1. In the top-left corner of the GUI, select **Action**, select **Change Password**, and then select **Change System Admin Password**.
2. In the **Change System Admin Password** dialog box, specify the required information, and then click **OK**.
3. Make sure that the processing results are correct, and then click **Close**.



Note:

- Specify a new password that meets the conditions set in the **Login Security** dialog box, such as the minimum number of characters and the combination of the characters that can be used as a password.
 - The password set here is required for the operation and management of the HDI system. Be sure not to forget this password.
 - The password is shared with the HDI API administrator account. If the password is changed from the GUI, use the new password in the API.
 - If the current password is lost, use the `adminpasswd` command to reset the password and then specify a new password.
-

Changing account security settings

You can change the session timeout time and the automatic account logout settings. You can also change the conditions for specifying the system administrator's password to prevent discovery by a third party. These conditions include the minimum number of characters and the combination of the characters that can be specified for the system administrator's password.

GUI used for this operation

- [Login Security dialog box on page C-38](#)

To change the account security settings

1. In the top-left corner of the GUI, select **Action**, and then **Login Security**.
2. In the **Login Security** dialog box, specify the required information, and then click **OK**.
3. Make sure that the processing results are correct, and then click **Close**.

Managing shared directories

This chapter describes how to manage shared directories.

- [Creating a shared directory](#)
- [Referencing other HDI data as read-only via the linked HCP](#)
- [Changing the policy and schedule for migrating data to HCP](#)
- [Setting conditions for preventing certain files from turning into stub files](#)
- [Expanding the capacity of a file system](#)
- [Importing data from another file server](#)

Creating a shared directory

This section explains how to create a shared directory.

GUI used for this operation

- [Create File System dialog box on page C-215](#)

To create a shared directory

1. In the top-left corner of the GUI, choose the **Resources** tab.
2. In the **General Tasks** area, click **Create File System**.
3. In the **Create File System** dialog box, specify a file system name, how to link to the HCP system, the access protocols to be used (CIFS, NFS, or both), the capacity, and other options.

Part of the specified size will be used as the work space for the Active File Migration function and the Large File Transfer function. The following table shows the size of the work space to be allocated for a specified file system capacity.

Table 3-1 Size of the work space to be used by the Active File Migration function and the Large File Transfer function

Capacity of the file system (m: capacity of the file system)	Capacity of the work space
100GB <= m <= 1TB	40GB
1TB < m <= 25TB	50GB
25TB < m <= 40TB	60GB
40TB < m	80GB

Table 3-2 Size of the work space to be used by the Active File Migration function (when the Large File Transfer function is not used)

Capacity of the file system (m: capacity of the file system)	Capacity of the work space
m < 4GB	0GB
4GB <= m <= 20GB	m / 2 (Values are rounded down to the nearest integer.)
20GB < m <= 17TB	10GB
17TB < m <= 256TB	25GB
256TB < m	25GB

Specify **File system** or **Subtree** for **Namespace type**, and then specify **Content sharing** to share data with other HDI systems via the linked HCP.

- If not synchronizing data with other HDI systems: Select **Off** for **Content sharing**. If you specify **File system** for **Namespace type**, also specify the quota to be allocated to the migration-destination namespace.
- If sharing data among HDI systems by using the read-write-content-sharing functionality: Select **On (Read/Write)** for **Content sharing**, and then specify the information about the migration-destination namespace. You must specify **File system** for **Namespace type**.
- If roaming among HDI systems is enabled for home directory data created for each end user: Select **Home directory** for **Content sharing**, and then specify the information about the migration-destination namespace. You must specify **File system** for **Namespace type** and specify **CIFS** for the access protocol.



Note: If a file system is linked to the HCP system at the share level, you cannot use the **Create File System** dialog box to create a share or allocate the namespace. After creating the file system, use the **Add Share** dialog box to add the file share directly below the mount point, and then allocate the namespace to the file share.

If you want to apply WORM to the files in the shared directory, enable **Enable the WORM function**. If the WORM function is enabled, any file can be prevented from being changed or deleted for a set period of time. However, if you specify **On (Read/Write)** or **Home directory** for **Content sharing**, you cannot enable the WORM functionality. Note that after enabling the WORM functionality, you cannot disable the WORM functionality.

To show clients previous data that was migrated to the HCP system, enable **Use file version restore** and specify how the previous data is to be kept.

To use CIFS bypass traverse checking, enable **CIFS bypass traverse checking**. However, if you specify **Home directory** for **Content sharing**, you cannot enable CIFS bypass traverse checking.

4. Click **OK**.
5. Verify the information displayed in the confirmation dialog box, and then click **Apply**.
6. Make sure that the processing results are correct, and then click **Close**.

Referencing other HDI data as read-only via the linked HCP

This section describes referencing other HDI data as read-only via the linked HCP.

GUI used for this operation

- [Create File System dialog box on page C-215](#)

To reference other HDI data as read-only via the linked HCP

1. In the top-left corner of the GUI, choose the **Resources** tab.
2. In the **General Tasks** area, click **Create File System**.
3. In the **Create File System** dialog box, specify a file system name, how to link to the HCP system, the access protocols to be used (CIFS, NFS, or both), and the capacity.



Note: If a file system is linked to the HCP system at the share level, you cannot use the **Create File System** dialog box to create a share or allocate the namespace. After creating the file system, use the **Add Share** dialog box to add the file share directly below the mount point, and then allocate the namespace to the file share.

4. Select **On (Read-Only)** for **Content sharing**.
5. If you select **File System** for **Namespace type**, specify the HCP namespace information that refers to the data.
Specify the system information for the HCP namespace whose data you want to show and specify a namespace-access account.
If you are using the replication functionality in the HCP system, also specify the system information for the replica HCP system.
Click **Test Connection** to check whether you can connect to the HCP.
6. Click **OK**.
7. Verify the information displayed in the confirmation dialog box, and then click **Apply**.
8. Make sure that the processing results are correct, and then click **Close**.

Changing the policy and schedule for migrating data to HCP

This section explains how to change the policy and schedule for migrating data to the HCP system.

GUI used for this operation

- [Migration Tasks dialog box on page C-4](#)
- [Migration Task Wizard on page C-15](#)

To edit the policy and schedule for migrating data to the HCP system

1. In the top-left corner of the GUI, select **Action**, and then **Migration Tasks**.
2. In the **Migration Tasks** dialog box, select the target task, and then click **Edit Task**.
3. In the **2. Task Settings** page in the **Migration Task Wizard**, specify the required information.
4. In the **3. Schedule Settings** page, specify the required information.
5. In the **4. Policy Settings** page, specify the required information.

If you do not specify a policy, all files will be migrated.

6. In the **5. Confirmation** page, select **I have confirmed the above settings.**, and then click **Apply**.

Setting conditions for preventing certain files from turning into stub files

This section explains how to set conditions (cache resident policies) so that certain files are not turned into stub files when the data in the file system is migrated to the HCP system.

After you set conditions for preventing certain files from turning into stub files, file data that satisfies the conditions is always retained in the HDI system (cache residency). This causes the access time for these files to be shorter than for stub files.

GUI used for this operation

- [file-system-name window on page C-61](#)
- [Add Cache Resident Policy dialog box on page C-237](#)

To set conditions for preventing certain files from turning into stub files

1. In the top-left corner of the GUI, choose the **Resources** tab.
2. In a tree on the left side of the GUI, select the triangle icon to the left of the *host-name*.
3. In a tree on the left side of the GUI, select the triangle icon to the left of **File Systems**, and then click a file system name.
4. In the *file-system-name* window, click the **Cache Resident Policy** tab.
5. In the **Cache Resident Policy** tab, click the **Add**.
6. In the **Add Cache Resident Policy** dialog box, specify the necessary information.



Tip: Only files that meet all the conditions set for a policy are prevented from being turned into stub files. If multiple policies are set up, a file is not turned into a stub file if all the conditions in at least one of the policies are met.

7. Click **OK**.
8. Verify the information displayed in the confirmation dialog box, and then click **Apply**.
9. Make sure that the processing results are correct, and then click **Close**.

After cache resident policies are set up, tasks for suppressing or recalling stub files are executed everyday at midnight to prevent the files that satisfy the specified conditions from turning into stub files.

Expanding the capacity of a file system

This section explains how to expand the capacity of a file system in which a shared directory was created.

If you want to expand the capacity of a volume group used by a file system, you need to increase the number of disks. For details about how to increase the number of disks, see [Increasing the number of disks on page 6-2](#).

GUI used for this operation

- [File Systems window on page C-56](#)
- [Edit File System dialog box on page C-228](#)

To expand the capacity of a file system

1. In the top-left corner of the GUI, choose the **Resources** tab.
2. In a tree on the left side of the GUI, select the triangle icon to the left of the *host-name*, and then click **File Systems**.
3. In the **File Systems** window, select the file system, and then click **Edit**.
4. In the **Edit File System** dialog box, specify the size in **Allocate capacity**.

Part of the specified size will be used as the work space for the Active File Migration function and the Large File Transfer function. For details about the size of the work space to be allocated for a specified file system capacity, see [Table 3-1 Size of the work space to be used by the Active File Migration function and the Large File Transfer function on page 3-2](#) or [Table 3-2 Size of the work space to be used by the Active File Migration function \(when the Large File Transfer function is not used\) on page 3-2](#).

5. Click **OK**.
6. Verify the information displayed in the confirmation dialog box, and then click **Apply**.
7. Make sure that the processing results are correct, and then click **Close**.

Importing data from another file server

This section describes how to use GUIs to import file shares data that is used in another file server to the HDI system. You can import data from multiple file servers at the same time. A maximum of 20 file shares can be imported at the same time per HDI system. The way of importing data depends on the protocol being used. If you use the CIFS protocol, see [Importing data from another file server by using the CIFS protocol on page 3-7](#). If you use the NFS protocol, see [Importing data from another file server by using the NFS protocol on page 3-11](#). If the share type of the import-source file server differs from the protocol used for importing data, information including the attribute might not be imported correctly. Use the same protocol as the share type when importing data. Note that import cannot be performed from a share that uses both the CIFS and NFS protocols.



Note: To set capacity limitations for each file share, user, or group, command settings are required when an importation starts. Therefore, we recommend you to use commands for importing data if you want to set capacity limitation. For details about how to use commands for importing data from another file server, see the *Cluster Administrator's Guide*.

Importing data from another file server by using the CIFS protocol

This section describes how to import data from another file server by using the CIFS protocol.

Before importing data, you must set the configuration definitions of the CIFS service. Only files that are in non-WORM file system and are accessed by CIFS clients can be imported. The directory path of each file must be no more than 4,095 bytes including the file name.

Before starting a data import operation, make sure that the import-source file server supports the versions of the SMB protocol that the CIFS service uses to communicate with file servers. If the file server does not support those versions of the SMB protocol, change the values specified for the options `client_max_protocol` and `client_min_protocol`, of the command `cifsopset`, that determine the versions of the SMB protocol that the CIFS service uses to communicate with the import-source file server.

The following information and objects are not imported:

- File system attributes such as quota and share settings
- Symbolic links
- SACL (System ACL) and quota information for files and directories
- Encryption, compression, and non-indexed attributes for files and directories (The settings are removed.)
- Accounts that are not registered on the domain controller and accounts other than `Everyone`, `CREATOR OWNER`, or `CREATOR GROUP` (when domain authentication is used)
- Accounts that cannot be resolved by HDI: accounts that are not registered in user mapping as trusted domains, original accounts for accounts that are transferred by using Active Directory domains, and deleted accounts
- The directories and files of the following names: `.history`, `.snaps`, `.arc`, `.system_gi`, `.system_reorganize`, `.backupupdates`, `.temp_backupupdates`, `lost+found`, `.lost+found`

System directories that are used by the server and that are in the import-source CIFS shares sometimes fail to be imported. If this happens, revise the owner accounts as well as any other accounts for which file access permissions for the directories that failed to be imported are set, and then perform the importation again.

No more than 700 ACEs set for files and directories can be imported. The imported files have archive attributes as DOS attributes. Also, the attributes for NTFS ACL are converted into the corresponding attributes for Advanced

ACL. For details about correspondence between NTFS ACL and Advanced ACL attributes, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

Before importation, download the Microsoft Visual C++ 2010 Redistributable Package (x86) from Microsoft Download Center, and then install it on the import-source file server.

For details about the user mapping method used when data is imported, see [Identifying users by user mapping on page 4-9](#).

GUI used for this operation

- [Import Files dialog box on page C-27](#)
- [List of RAS Information page on page C-39](#)
- [Shares window on page C-53](#)
- [Local Users dialog box on page C-85](#)
- [DNS, NIS, LDAP Setup page on page C-117](#)
- [Create File System dialog box on page C-215](#)

To import data from another file server by using the CIFS protocol

1. Create a data access account for importation.
Create an account for accessing shared data in an external authentication server. Set up an account so that the account can access all data in the shares to be imported. Specify the account name using no more than 256 characters and the password using no more than 128 characters. You can use alphanumeric characters, sign characters except backslashes (\), and multi-byte characters that are encoded in UTF-8.
2. If import-target files exist for which the owners or ACLs are local accounts or accounts that are not resolved by HDI, on the import-source file server, verify the local accounts, and then create a mapping file for using the accounts in the HDI system.

For Microsoft(R) Windows Server(R), use the mapping generation tool (`sidlist.exe`) to create a mapping file. The mapping generation tool is stored at the following location on the HDI installation media.

installation-media-drive: \tool\sidlist

Copy `sidlist.exe` to a desired directory on the import-source file server, and then run it by specifying the absolute path of `sidlist.exe` and the mapping file.

Example for when `sidlist.exe` is stored in the `tool` directory on the `D` drive:

```
D:\>d:\tool\sidlist.exe >d:\tool\mappingfile.txt
```

Verify the character encoding of the mapping file, and then save the file in the UTF-8 format.

The entries are output to a mapping file as follows:

```
[MAPDEF]
SID=account-SID
```

```
SRC_NAME=import-source-account-name
KIND=account-type (u (user) or g (group))
DST_NAME=import-target-account-name
```

If you want to use different account names in the HDI system than the ones that have been used on the import-source file server, edit the `DST_NAME` for those accounts. If you use domain accounts, specify the names in *domain-name\account-name* format.

For servers other than Microsoft(R) Windows Server(R), manually create a mapping file containing the above entries for each local account.

Verify the character encoding of the mapping file (use UTF-8).

3. Connect the HDI system to the network in which the HDI system can access the import-source file server.
4. Perform the necessary settings depending on how the import-source files will be accessed.

When domain authentication is used

Set the same DNS, NIS, and LDAP information for the HDI system as the one set for the import-source file server.

Set the information so that the name resolution and user authentication work when clients access the HDI system in the same way as when clients access the import-source file server. Also set up user and group mapping by the external authentication server.

When local authentication is used

Register the local accounts that were used on the import-source file server to the HDI system.

Register the users and groups by using the names for `DST_NAME` in step 2 and specifying desired UIDs and GIDs.

When both domain authentication and local authentication are used

Perform the settings necessary for both domain authentication and local authentication.

5. Create and share the import-target file system in the HDI system.
Note that this step is unnecessary if the import-target file system and file share have already been created.

Create a non-WORM file system.


In addition, set information about the namespace and a migration schedule. Content sharing must be set to off.

If you want to migrate data that is stored in the file system and updated during an importation to an HCP, configure settings to periodically migrate the data. However, if data migration starts during an importation, importation of all data is temporarily stopped, and then the importation method is changed to on-demand. This increases the time needed for importing data. To reduce the time needed for importing data, set a migration schedule in step 18 after the importation is completed.


Do not create any files or directories in the import-target file system until a importation is started in step 14. If a file or directory path is the same as one in the import-source file system, the file or directory

corresponding to that path in the import-source file system is not imported.

6. In the **Shares** window, select the shared directory created in step 5, and then click **Import Files**.
7. In the **Import Files** dialog box, specify the necessary information, and then click **Show Plan**.
8. Make sure that the information displayed in the confirmation dialog box is correct, and then click **Start Scan**.
Make sure that verification of the import-source files has started, and, if necessary, click **Close**.
9. In the top-left corner of the GUI, select the **Tasks** tab.
The **Import Files** window appears.
10. In the **Import Files** window, check the status of the defined tasks.
Make sure that **Status** is `Scan finished`.

If the Caution icon () is displayed, an error occurred during verification, or some files could not be recognized as verification targets. Click the task name, and display the **Import Files** dialog box. In the dialog box, click **Display Scan Failure List** or **Display Read Failure List**, and check the details about the error. Also, take any necessary action.

11. Notify clients who are using the import-source file server of the importation schedule.
12. Set shares in the import-source file server as read-only.
If an import-source file or directory is updated after the import starts, the file or directory might not be properly imported.
13. Use MMC (Microsoft Management Console) (or some other similar tool) to disconnect the session connected to the import-source file server.
For details about how to disconnect sessions, see the documentation for the import-source file server.
14. In the **Import Files** window, select a task, and then click **Start Import**.
15. Make sure that the information displayed in the confirmation dialog box is correct, and then click **Apply**.
16. Inform clients that they can start accessing shares in the HDI system.
Clients can access the shares in the HDI system during data importation. To check the progress of the import, from the **Tasks** tab, check the **Import Files** window. In the **Import Files** window, `Import finished` is displayed for **Status** if the import is completed.
17. In the **Import Files** window, check the results of the import.

If the Caution icon () is displayed, an error occurred during the import, or some files could not be recognized as import sources. Click the task name, and display the **Import Files** dialog box. In the dialog box, click **Display Import Failure List** or **Display Read Failure List**, and check the details about the error.

If files or directories are moved while a importation is being performed, those files might not have been imported. Confirm that all the files were imported.

If importation failed for some files, take action according to the recovery procedure described in the *Single Node Troubleshooting Guide*.

If no files failed, but the number of import-source files differs from the number of files that were successfully imported, redo this procedure from step 14. The files that were not imported will be imported.

If a node failure occurs or the file system capacity is insufficient while importing data from another file server, the import process might fail. If this happens, a message is still output to prompt users to import data again even after an all-file import is performed again. Run the `datamigratestatus` command with the `--incompletionlist` option to verify that the displayed files are all imported. If the files have been imported, no action is necessary. If some files have not been imported, take action by, for example, manually copying the files one-by-one.

18. Set a migration schedule.

Configure this setting if the schedule is not set in step 5. If a migration schedule is set in step 5 and migration has never been performed, execute the `arcmodectl` command with the `--init-migration enable` option specified to enable the initial mode. If 1,000,000 or more files are to be imported, execute the `arcmodectl` command with the `--init-migration enable` and `-t repeat` options specified to enable initial mode every time a task is executed. If you specify the `-t repeat` option, when the number of files to be migrated drops below 1,000,000, disable initial mode.

19. Remove the import-source file server.

If a failure occurred during data importation, take action according to the recovery procedure described in the *Single Node Troubleshooting Guide*.

Importing data from another file server by using the NFS protocol

This section describes how to import data from another file server by using the NFS protocol.

Before importing data, you must set the configuration definitions of the NFS service on the node. Only files that are in non-WORM file systems and are accessed by NFS clients can be imported. The directory path of each file must be no more than 4,095 characters, including the file name.

The following information and objects are not imported:

- Quota information and ACL for files and directories
- File system attributes such as quota and share settings
- Socket files
- The directories and files of the following names: `.history`, `.snaps`, `.arc`, `.system_gi`, `.system_reorganize`, `.backupdates`, `.temp_backupupdates`, `lost+found`, `.lost+found`

GUI used for this operation

- [Import Files dialog box on page C-27](#)


- [List of RAS Information page on page C-39](#)
- [Shares window on page C-53](#)
- [DNS, NIS, LDAP Setup page on page C-117](#)
- [Create File System dialog box on page C-215](#)

To import data from another file server by using the NFS protocol


1. Connect the HDI system to the network in which the HDI system can access the import-source file server.
2. Set the same DNS, NIS, and LDAP information for the HDI system as set for the import-source file server.
Configure the settings so that name resolution and user authentication used when a client accesses to the HDI system will operate in the same way as when a client accesses the import-source file server.
3. Configure the shared directory on the import-source file server so that the directory can be accessed from the HDI system.
 - Set the HDI IP address as a client that can access the shared directory.
 - Set the directory as read-only, and enable clients to access the directory by using the root permissions that clients start with.
4. Create and share the import-target file system in the HDI system.
Note that this step is unnecessary if the import-target file system and file share have already been created.
Create a non-WORM file system.
In addition, set information about the namespace and a migration schedule. Content sharing must be set to off.
If you want to migrate data that is stored in the file system and updated during an importation to an HCP, configure settings to periodically migrate the data. However, if data migration starts during an importation, importation of all data is temporarily stopped, and then the importation method is changed to on-demand. This increases the time needed for importing data. To reduce the time needed for importing data, set a migration schedule in step 16 after the importation is completed.
Do not create any files or directories in the import-target file system until an import is started in step 12. If a file or directory path is the same as one in the import-source file system, the file or directory corresponding to that path in the import-source file system is not imported.
5. In the **Shares** window, select the shared directory created in step 4, and then click **Import Files**.
6. In the **Import Files** dialog box, specify the necessary information, and then click **Show Plan**.
7. Make sure that the information displayed in the confirmation dialog box is correct, and then click **Start Scan**.
Make sure that verification of the import-source files has started, and, if necessary, click **Close**.
8. In the top-left corner of the GUI, select the **Tasks** tab.

The **Import Files** window appears.

9. In the **Import Files** window, check the status of the defined tasks. Make sure that **Status** is `Scan finished`.

If the Caution icon () is displayed, an error occurred during verification, or some files could not be recognized as verification targets. Click the task name, and display the **Import Files** dialog box. In the dialog box, click **Display Scan Failure List** or **Display Read Failure List** and check the details about the error. Also, take any necessary action.

10. Notify clients who are using the import-source file server of the importation schedule.
11. Set shares in the import-source file server as read-only.
If an import-source file or directory is updated after the import starts, the file or directory might not be properly imported.
12. In the **Import Files** window, select a task, and then click **Start Import**.
13. Make sure that the information displayed in the confirmation dialog box is correct, and then click **Apply**.
14. Inform clients that they can start accessing shares in the HDI system.
Clients can access the shares in the HDI system during data importation. To check the progress of the import, from the **Tasks** tab, check the **Import Files** window. In the **Import Files** window, `Import finished` is displayed for **Status** if the import is completed.
15. In the **Import Files** window, check the results of the import.

If the Caution icon () is displayed, an error occurred during the import, or some files could not be recognized as import sources. Click the task name, and display the **Import Files** dialog box. In the dialog box, click **Display Import Failure List** or **Display Read Failure List**, and check the details about the error.

If files or directories are moved while a importation is being performed, those files might not have been imported. Confirm that all the files were imported.

If importation failed for some files, take action according to the recovery procedure described in the *Single Node Troubleshooting Guide*.

If no files failed, but the number of import-source files differs from the number of files that were successfully imported, redo this procedure from step 12. The files that were not imported will be imported.

If a node failure occurs or the file system capacity is insufficient while importing data from another file server, the import process might fail. If this happens, a message is still output to prompt users to import data again even after an all-file import is performed again. Run the `datamigratestatus` command with the `--incompletionlist` option to verify that the displayed files are all imported. If the files have been imported, no action is necessary. If some files have not been imported, take action by, for example, manually copying the files one-by-one. Note that, if hard links for which different subtree quotas are set have not been imported to the import source and import target, check, and if necessary, revise the quota settings, and then create hard links for each.

16. Set a migration schedule.

Configure this setting if the schedule is not set in step 4. If a migration schedule is set in step 4 and migration has never been performed, execute the `arcmodectl` command with the `--init-migration enable` option specified to enable the initial mode. If 1,000,000 or more files are to be imported, execute the `arcmodectl` command with the `--init-migration enable` and `-t repeat` options specified to enable initial mode every time a task is executed. If you specify the `-t repeat` option, when the number of files to be migrated drops below 1,000,000, disable initial mode.

17. Remove the import-source file server.

If a failure occurred during data importation, take action according to the recovery procedure described in the *Single Node Troubleshooting Guide*.

Setting up the access environment from clients

This chapter describes how to set up the HDI system regarding the access environment from clients that use shared directories.

- [Setting up the access environment from CIFS clients](#)
- [Identifying users by user mapping](#)
- [Collecting CIFS client access logs](#)
- [Setting up the access environment from NFS clients](#)

Setting up the access environment from CIFS clients

This section describes how CIFS client access environments are applied to systems according to the network model that is used.

Joining a node to an Active Directory domain

A node can join an Active Directory domain to allow users belonging to the same domain or trusted domains to access HDI shared directories.

Prerequisites for joining a node to an Active Directory domain

Acquire the following Active Directory domain information that will be used during the joining procedure:

- DNS name and NetBIOS name of the domain that the node is joining
- Domain controller server name. Another name (alias) cannot be specified.
- Name and password of the domain controller user
- IP address of the DNS server used by the domain

Make sure that the DNS server used by the domain is configured as follows:

- IP addresses for the node and the corresponding host names have been registered.
- The SRV records required for deploying the Active Directory service have been registered.
- All the IP addresses registered for the host names of the domain controllers can be used to communicate with the node.
- An IP address is not dynamically added to the host name for the domain controller.

If all the following conditions are satisfied, edit the `/etc/cifs/lmhosts` file on the **Edit System File** page in the **Network & System Configuration** dialog box so that the nodes can search for the domain controller of the domain with which a trust relationship has been established:

- The domain to which the node belongs has a trust relationship with another domain.
- Either the domain to which the node belongs or a domain with which the node has a trust relationship is an NT domain.
- The node and a domain that has a trust relationship with the node exist on different network segments.

In the HDI system, create a shared folder that can use the CIFS protocol.


Make sure that the domain controller supports the versions of the SMB protocol that the CIFS service uses to communicate with the domain controller. If it does not support those versions of the SMB protocol, change the values specified for the options `client_ipc_max_protocol` and `client_ipc_min_protocol`, of the command `cifsoptset`, that determine the

versions of the SMB protocol that the CIFS service uses to communicate with the domain controller.

GUI used for this operation

- [host-name window on page C-51](#)
- [System Setup Menu page on page C-103](#)
- [DNS, NIS, LDAP Setup page on page C-117](#)
- [List of Services page on page C-137](#)
- [CIFS Service Management \(Basic\) page on page C-141](#)
- [Select Authentication Mode page on page C-157](#)
- [Active Directory Authentication page on page C-159](#)

To join a node to an Active Directory domain

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** in the **Setting Type** drop-down list, and then click **Display**.
5. In the **System Setup Menu** page (**Setting Type**: *network*), click **DNS, NIS, LDAP Setup**.
6. In the **DNS, NIS, LDAP Setup** page, specify information about the DNS server used for the Active Directory domain, and click **OK**.
If a confirmation dialog box is displayed, click **OK**.
7. In the **System Setup Menu** page, click **Close**.
8. From the *host-name* window, click **Access Protocol Configuration** in the **Settings** area.
9. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS**, and then click **Modify Configuration**.
10. In the **CIFS Service Management (Basic)** page, click **Change Authentication Mode**.
11. In the **Select Authentication Mode** page, select **Active Directory authentication** from the options, and then click **OK**.
12. In the **Active Directory Authentication** page, specify the necessary information, and then click **OK**.
13. On the **CIFS Service Management (Basic)** page, click **OK**.
14. On each page of **CIFS Service Management**, specify the necessary information, and then click **OK**.
Select the **Setting Type** drop-down list, and click **Display** for the necessary information. If you change **Setting Type**, click **OK** after specifying information.

When an Active Directory domain is joined, we recommend that you use user mapping to manage user information. For details about how to use user mapping, see [Identifying users by user mapping on page 4-9](#).

15. Click **End of Settings** on the confirm settings page.
16. On the **List of Services** page, restart the CIFS service. Also restart the NFS, FTP, or SFTP service as needed.
Inform any clients using the service of the temporary stoppage before starting. Select the target service and click **Restart** to restart the service. For details about whether the NFS, FTP, and SFTP services need to be restarted, see [Conditions that the NFS, FTP, and SFTP services need to be restarted on page 4-5](#).
17. Restart the node.

Notes on after joining a node to an Active Directory domain

- If the Active Directory authentication is set, make sure that the system times of the domain controller, the HDI system, and CIFS clients are the same. If there is a time difference of more than 5 minutes among these systems, authentication might fail when CIFS clients access the HDI system.
- After changing the Active Directory domain, if you immediately change the settings to rejoin the nodes to their previous Active Directory domain, authentication of a CIFS client might result in an error even though the processing was successful. In this case, in the **CIFS Service Maintenance** page, click **Rejoin Active Directory Domain** to rejoin the nodes to the Active Directory domain.
- If you join the nodes to another Active Directory domain that has the same name as the previous one, an unnecessary computer account might remain in the previous Active Directory domain. Use the domain controller of the previous Active Directory domain to delete the unnecessary computer account.
- When a user registered in a domain attempts to access the CIFS share of an HDI system from a client machine that is not registered in the domain, user authentication might fail. In this case, use the **CIFS Service Maintenance** page to check whether the NetBIOS name of the Active Directory domain has been set correctly.
- If Active Directory is used for user authentication, only users authenticated by Active Directory can access CIFS shares. Users locally authenticated by the HDI system cannot access CIFS shares.
- If you change settings that specify the SMB protocols supported by the domain controller, an error might occur during CIFS client authentication. If this occurs, make sure that the domain controller supports the versions of the SMB protocol that the CIFS service uses to communicate with the controller. If it does not support those versions of the SMB protocol, change the values specified for the options `client_ipc_max_protocol` and `client_ipc_min_protocol`, of the command `cifsoptset`, that determine the versions of the SMB protocol that the CIFS service uses to communicate with the domain controller.

Conditions that the NFS, FTP, and SFTP services need to be restarted

The NFS service needs to be restarted in the following cases.

- When using an Active Directory domain controller and KDC server together, and a different name is set than that of the domain to which the KDC server using the NFS service belongs, or that of the KDC server

The FTP or SFTP service needs to be restarted in the following cases.

- If the FTP or SFTP service settings allow users authenticated with Active Directory to log on, and the authentication type is changed from Active Directory to another type or from another type to Active Directory.


Rejoining an Active Directory domain

If a domain controller failure or a domain configuration change occurs while Active Directory is being joined, connection to the CIFS share might not be possible. In this case, the node can join the Active Directory domain again to restore the connection to the CIFS share.

GUI used for this operation

- [host-name window on page C-51](#)
- [List of Services page on page C-137](#)
- [CIFS Service Maintenance page on page C-177](#)

To rejoin an Active Directory domain

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Access Protocol Configuration** in the **Settings** area.
4. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS**, and then click **Service Maintenance**.
5. In the **CIFS Service Maintenance** page, click **Rejoin Active Directory Domain**.

The selected CIFS service is rejoined to the Active Directory domain.



Note: If an attempt to rejoin the Active Directory domain fails, manually delete any computer accounts remaining on the Active Directory domain, and try again.

Joining a node to an NT domain

A node can join an NT domain to allow users belonging to the same domain or trusted domains to access HDI shared directories.

Prerequisites for joining a node to an NT domain

Acquire the following NT domain information that will be used during the joining procedure:

- DNS name and NetBIOS name of the domain that the node is joining
- Domain controller server name. Another name (alias) cannot be specified.
- User name and password of the domain controller administrator
- IP address of the DNS server used by the domain

If all the following conditions are satisfied, edit the `/etc/cifs/lmhosts` file on the **Edit System File** page in the **Network & System Configuration** dialog box so that the nodes can search for the domain controller of the domain with which a trust relationship has been established:

- The domain to which the node belongs has a trust relationship with another domain.
- Either the domain to which the node belongs or a domain with which the node has a trust relationship is an NT domain.
- The node and a domain that has a trust relationship with the node exist on different network segments.


Make sure that the network segment to which the node is connected does not contain computers that are not servers and whose names are the same as the domain controller server name specified in the **NT Domain Authentication** page. When the nodes are connected to multiple network segments (including VLANs), check the above condition for all the network segments to be connected.

In the HDI system, create a shared folder that can use the CIFS protocol.

GUI used for this operation

- [host-name window on page C-51](#)
- [List of Services page on page C-137](#)
- [CIFS Service Management \(Basic\) page on page C-141](#)
- [Select Authentication Mode page on page C-157](#)
- [NT Domain Authentication page on page C-158](#)

To join a node to an NT domain

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Access Protocol Configuration** in the **Settings** area.
4. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS** from the options, and then click **Modify Configuration**.

5. In the **CIFS Service Management (Basic)** page, click **Change Authentication Mode**.
6. In the **Select Authentication Mode** page, select **NT domain authentication** from the options, and then click **OK**.
7. On the **NT Domain Authentication** page, specify the necessary information, and then click **OK**.
8. On the **CIFS Service Management (Basic)** page, click **OK**.
9. On each page of **CIFS Service Management**, specify the necessary information, and then click **OK**.
 Select the **Setting Type** drop-down list, and click **Display** for the necessary information. If you change **Setting Type**, click **OK** after specifying the information.
 When an NT domain is joined, we recommend that you use user mapping to manage user information. For details about how to use user mapping, see [Identifying users by user mapping on page 4-9](#).
10. Click **End of Settings** on the settings confirmation page.
11. In the **List of Services** page, restart the CIFS service. Also, restart the FTP or SFTP service as needed.
 Inform any clients using the service of the temporary stoppage before starting. Select the target service and click **Restart** to restart the service. The FTP or SFTP service needs to be restarted if the FTP or SFTP service settings allow users authenticated with Active Directory to log on, and the authentication type is changed from Active Directory.
12. Restart the node.


Configuring a workgroup

In a workgroup, nodes authenticate users who access nodes.

GUI used for this operation

- [host-name window on page C-51](#)
- [List of Users / Groups page on page C-85](#)
- [Add User page on page C-88](#)
- [Add Group page on page C-96](#)
- [List of Services page on page C-137](#)
- [CIFS Service Management \(Basic\) page on page C-141](#)
- [Select Authentication Mode page on page C-157](#)
- [Local Authentication page on page C-158](#)

To configure a workgroup

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .

3. From the *host-name* window, click **Access Protocol Configuration** in the **Settings** area.
4. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS** from the options, and then click **Modify Configuration**.
5. In the **CIFS Service Management (Basic)** page, click **Change Authentication Mode**.
6. In the **Select Authentication Mode** page, select **Local authentication** from the options, and then click **OK**.
7. In the **Local Authentication** page, specify the necessary information, and then click **OK**.
8. On the **CIFS Service Management (Basic)** page, click **OK**.
9. On each page of **CIFS Service Management**, specify the necessary information, and then click **OK**.
Select the **Setting Type** drop-down list, and click **Display**, for the necessary information. If you change **Setting Type**, click **OK** after specifying the information.
10. Click **End of Settings** on the settings confirmation page.
11. In the **List of Services** page, restart the CIFS service. Also, restart the FTP or SFTP service as needed.
Inform any clients using the service of the temporary stoppage before starting. Select the service to be restarted and click **Restart** to restart the service. The FTP or SFTP service needs to be restarted if the FTP or SFTP service settings allow users authenticated with Active Directory to log on, and the authentication type is changed from Active Directory.
12. Restart the node.
13. From the *host-name* window, click **Local Users** in the **Settings** area.
14. On the **List of Users / Groups** page (for *List of users*) of the **Local Users** dialog box, select **List of groups** from the drop-down list, and then click **Display**.
15. On the **List of Users / Groups** page (for *List of groups*), click **Add New Group**.
16. On the **Add Group** page, add groups that access shared directories on the node, and then click **OK**.
To enable the group to access CIFS shared directories, select **Apply to CIFS ACL environment**.
17. On the **List of Users / Groups** page (for *List of groups*), select **List of users** from the drop-down list, and then click **Display**.
18. On the **List of Users / Groups** page (for *List of users*), click **Add New User**.
19. On the **Add User** page, add users that access shared directories on the node, and then click **OK**.
To enable the user to access CIFS shared directories, select **Apply to CIFS environment**.

Identifying users by user mapping

When user mapping is used, since the user ID and group ID are assigned for the CIFS clients managed by the Active Directory domain and NT domain, the HDI system can identify users.

User-mapping methods

User mapping using RIDs

When a CIFS client accesses the HDI file system, the RIDs (relative identifiers) comprising the SID are converted, and the user ID and group ID are automatically assigned.

User mapping using LDAP

User IDs and group IDs are assigned according to the user information registered in the LDAP server database. These can be registered manually in advance, or automatically in the LDAP server database when a CIFS client accesses the HDI.

User mapping using Active Directory schema

When Active Directory authentication is used, correspondence for different identify IDs between NFS clients and CIFS clients can be managed as a user attribute. User IDs and group IDs are assigned according to the user information already registered in the domain controller.

Prerequisites for user mapping


- To change the user mapping method that you use, you need to re-create the file systems after you migrate the data by using Windows backup function.
- When a user ID or group ID is assigned, it can no longer be reused, even if you delete the user information from the domain controller.
- Make sure that the user IDs and group IDs used for user mapping do not overlap with those registered for the HDI system, NIS server, or user authentication LDAP server.
- If the RID or LDAP method is used to automatically assign user IDs and group IDs, the range of used IDs is reserved. The ID range can only have the maximum value changed. To prevent the ID range used for user mapping from becoming non-extensible due to overlap with IDs registered for the HDI system, NIS server, or user authentication LDAP server, we recommend that numerical IDs larger than those used for user mapping not be used for the HDI system, NIS server, or user authentication LDAP server.
- When using LDAP user mapping, create a tree on the LDAP server that contains the user IDs and group IDs, before performing HDI settings.

GUI used for this operation

- [host-name window on page C-51](#)

- [List of Services page on page C-137](#)
- [CIFS Service Management \(Basic\) page on page C-141](#)
- [CIFS Service Management \(User mapping\) page on page C-143](#)

To use user mapping

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Access Protocol Configuration** in the **Settings** area.
4. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS**, and then click **Modify Configuration**.
5. Select **User mapping** from the **Setting Type** drop-down list on the **CIFS Service Management (Basic)** page, and click **Display**.
6. On the **CIFS Service Management (User mapping)** page, specify the necessary information, and click **OK**.
7. Click **End of Settings** on the settings confirmation page.
8. Restart the CIFS service.
Inform any clients using the service of the temporary stoppage before starting. Select the target service and click the **Restart** to restart the service.



Note:

- Even if a user registered by the domain controller is registered with the same name as for the HDI, the NIS server, or the LDAP server for user authentication, the user ID and group ID assigned by user mapping will be used when the user accesses a CIFS share.
 - You can use commands to view information about users and groups mapped by the RID method. For details about how to view user mapping information, see the *CLI Administrator's Guide*.
-

Collecting CIFS client access logs


You can specify when CIFS client access logs (CIFS access logs) should be collected.

Specified settings are applied to the entire CIFS service. However, if events that are recorded as the CIFS access log are specified for each CIFS share by using the `cifscreate` command or the `cifsedit` command, the settings for each CIFS share are given priority over the settings for the entire CIFS service. When the settings for the CIFS service are changed, verify the settings for each CIFS share as well as the settings for the entire CIFS service.

GUI used for this operation

- [host-name window on page C-51](#)
- [List of Services page on page C-137](#)
- [CIFS Service Management \(Basic\) page on page C-141](#)
- [CIFS Service Management \(Security\) page on page C-149](#)
- [Setting Events Logged to the CIFS Access Log page on page C-161](#)

To collect CIFS client access logs

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Access Protocol Configuration** in the **Settings** area.
4. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **CIFS** from the options, and then click **Modify Configuration**.
5. Select **Security** from the **Setting Type** drop-down list in the **CIFS Service Management (Basic)** page, and click **Display**.
6. In the **CIFS Service Management (Security)** page, select **Use for CIFS access log**, and then click **Set Up** in **Events logged to the CIFS access log**.
7. In the **Setting Events Logged to the CIFS Access Log** page, select events that you want to record as the CIFS access log, and then click **OK**.
8. Click **OK** on the **CIFS Service Management (Security)** page.
9. Click **End of Settings** on the settings confirmation page.

Setting up the access environment from NFS clients


This section explains how to enable NFS clients to access shared directories.

If Kerberos authentication is used, set up an NTP server to synchronize the times of the HDI system and the NFS client hosts.

GUI used for this operation

- [host-name window on page C-51](#)
- [List of Services page on page C-137](#)
- [NFS Service Management page on page C-168](#)

To enable NFS clients to access shared directories

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .

3. From the *host-name* window, click **Access Protocol Configuration** in the **Settings** area.
4. In the **List of Services** page of the **Access Protocol Configuration** dialog box, select **NFS** from the options, and then click **Modify Configuration**.
5. In the **NFS Service Management** page, specify the required information, and then click **OK**.
6. In the **List of Services** page, select **NFS**, and then click **Restart** to restart the NFS service.

Showing previous data

This chapter describes how to show clients the previous data of files in shared directories.

- [Showing previous data on HCP](#)

Showing previous data on HCP

This section explains how to show clients previous data that was migrated to the HCP system.

GUI used for this operation

- [File Systems window on page C-56](#)
- [Edit File System dialog box on page C-228](#)

To show previous data on HCP

1. In the top-left corner of the GUI, choose the **Resources** tab.
2. In a tree on the left side of the GUI, select the triangle icon to the left of the *host-name*, and then click **File Systems**.
3. In the **File Systems** window, select the target file system, and then click **Edit**.
4. In the **Edit File System** dialog box, select **Yes** for **Use file version restore**, and then specify how the previous data is to be kept.
5. Click **OK**.
6. Verify the information displayed in the confirmation dialog box, and then click **Apply**.
7. Make sure that the processing results are correct, and then click **Close**.
8. Change the CIFS client settings for the shared directory so that all files and folders are displayed.

This allows CIFS clients to view to the `.history` folder in the shared directory in which previous data is shown.

Managing disk capacity

This chapter describes how to manage disk capacity.

Use commands to manager disk capacity. See [Setting up the SSH environment to use commands on page 11-2](#) to set up a proper environment.

- [Increasing the number of disks](#)
- [Changing the use of disks](#)

Increasing the number of disks

This section describes how to increase the number of disks that can be assigned to a file system to create or expand a volume group that can be used for the file system. Work with maintenance personnel or the storage system administrator to perform this task.



Tip: A maximum of 32 MB is used as a management area per LU. Therefore, the total capacity of a volume group differs from the total capacity of internal hard disks or storage system's LUs.

For details about how to add internal hard disks to a node, see [Adding internal hard disks to a node on page 6-2](#). For details about how to add LUs to a running storage system, see [Adding LUs to a running storage system on page 6-3](#).

Adding internal hard disks to a node

This section describes how to add internal hard disks to a node to increase the number of disks.

To add internal hard disk to a node

1. Notify clients of a temporary stoppage of the service.
2. Execute the `nasshutdown` command to stop the OS running on the node.
3. Add disks to the node.
4. Use the node power switch to turn on the node.

For details about the node power switch, see [Starting and forcibly stopping a node OS on page H-2](#).

5. Execute the `lumaplist` command and then the `hwstatus` command to check the status of the internal hard disks.
Make sure that the disks have been added and no problem has occurred on the disks.

6. From a browser, log on to the system.
A dialog box appears that asks you whether to automatically assign the added disks to a volume group.

7. Click **Yes**.
The added disks are automatically assigned to an existing or created volume group.
If there is a volume group with the same drive type as that of the disks added to the internal hard disk, the disks are assigned to the volume group. For other cases, a volume group is created for each drive type with a different name (`vg four-digit-number`) from those of the existing volume groups.



Tip: If you click **No**, you need to use the `vgcreate` command to create a volume group to which the disks are to be assigned or to use the `vgexpand` command to assign the disks to an existing volume group.

8. Make sure that the processing results are correct, and then click **Close**.

Adding LUs to a running storage system

This section describes how to add LUs to a running storage system to increase the number of disks.

Before adding LUs to a running storage system to increase the number of disks

If you are using the LUs of the target storage system on HDI for the first time, perform the following procedure first:

1. Ask the administrator of the storage system to set the host group and the paths for the LUs on the storage system side.
2. If HDI and the storage system are not connected, work with the administrator of the storage system to connect HDI and the storage system.

If you connected HDI and the storage system before configuring the settings on the storage system side, perform one of the following:

- Disconnect and then reconnect the FC cable that connects the node and the storage system.
- Disable and then re-enable the port connected to the storage system on the FC switch located between the node and the storage system.
- Restart the node.

To add LUs to a running storage system

1. Ask the storage system's administrator to create LUs to be used in the HDI system and to add the paths for the LUs.
2. Execute the `lumaplist` command to view the LU information.
If a problem occurs with the LU paths, contact the storage system administrator.
3. From a browser, log on to the system.
A dialog box appears that asks you whether to automatically assign the added LUs to a volume group.
4. Click **Yes**.

The added LUs are automatically assigned to an existing or created volume group.

If there is a volume group with the same drive type (same pool for virtual LUs) as that of the LUs added to the same storage system, the LUs are assigned to the volume group. For other cases, a volume group is created for each drive type (pool for virtual LUs) with a different name (`vgfour-digit-number`) from those of the existing volume groups.



Tip: If you click **No**, you need to use the `vgrcreate` command to create a volume group to which the LUs are to be assigned or to use the `vgexpand` command to assign the LUs to an existing volume group.

5. Make sure that the processing results are correct, and then click **Close**.

Changing the use of disks

This section explains how to perform the necessary tasks when changing the use of disks for an HDI system.

Deleting a volume group

This section explains how to delete a volume group. When using a storage system, perform the operation together with the storage system administrator.

To delete a volume group

1. Delete all file systems using the target volume group.
2. Execute the `vgrdelete` command to delete the target volume group.
3. When using a storage system, ask the storage administrator to delete the LU paths.
Delete the paths to all the LUs that make up the volume group.
4. Execute the `lumaplist` command to view the LU information.
If a problem occurs with the LU paths, contact the storage system administrator.

Deleting LUs that are not being used by file systems from a volume group

This section explains how to delete LUs from a volume group when using a storage system. You can delete only LUs that are not being used by file systems. Perform this operation together with the storage system administrator.

To delete LUs that are not being used by file systems from a volume group

1. Execute the `lumaplist` command with the `-v` option specified, and then confirm the name of the volume group assigned to the LU.
2. Execute the `vgrrepair` command with `--list` and `--lu` options specified, and then confirm that the LU is not used by the file system.
3. Ask the storage system administrator to delete the LU path.
4. Execute the `vgrrepair` command to repair the volume group.
5. Execute the `lumaplist` command to view the LU information.

If a problem occurs with the LU paths, contact the storage system administrator.

Protecting user data

This chapter describes how to set up virus scanning and back up and restore user data.

- [Setting up virus scanning](#)
- [Backing up data to a tape device](#)
- [Restoring data from a tape device](#)


Setting up virus scanning

This section explains how to set up virus scanning that is performed when CIFS clients access files.

GUI used for this operation

- [host-name window on page C-51](#)
- [List of Scanner Servers page on page C-186](#)
- [Add Scanner Server page on page C-189](#)
- [Scan Conditions page on page C-190](#)
- [Scanning software page on page C-196](#)

To set up virus scanning

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Virus Scan Server Configuration** in the **Settings** area.
4. On the **List of Scanner Servers** page of the **Virus Scan Server Configuration** dialog box, click **Scanning Software**.
5. On the **Scanning software** page, select the desired software, and then click **OK**.
6. On the **List of Scanner Servers** page, click **Add Server**.
7. On the **Add Scanner Server** page, specify the IP address, domain name, or host name of the scan server, and a port number of the scan server, and then click **Add**.
8. On the **List of Scanner Servers** page, click **Scan Conditions**.
9. View the **Scan Conditions** page, change settings as necessary, and click **OK**.



Note: After you enable the scanning, restart the CIFS service.

Backing up data to a tape device

This section explains how to back up data to a tape device.

If either of the following conditions is met, backup processing might end with an error:

- The total size of the length of the directory and file names to be backed up at the same time exceeds 1 GB.
- The total size of the length of the directory and file names in the directory immediately under the directories to be backed up at the same time exceeds 1 GB.

When calculating the sum, add 1 byte as the delimiter between each directory and file.

Make sure the total length of the names of the directories and files to be backed up does not exceed 1 GB by reducing the number of directories and files to be backed up, or by adjusting the hierarchy.

To back up data to a tape device

1. Estimate the required backup media capacity.
Estimate the required backup media capacity from the amount of data to be backed up, and then prepare a tape device. For details on how to estimate the backup media capacity, see the *Installation and Configuration Guide*.
2. Set up the operating environment for the backup management software.
For details on how to set up an operating environment for the backup management software, see Backup Restore, supplementary material provided with the HDI system.



Note: Some backup management software products might not work correctly if the length of the path for data to be backed up is too long. Before starting formal operations, perform a test to make sure that backup and restore operations are performed correctly.

If the interruption for an offline backup is configured so that backup processing continues even if a file is modified or deleted during the offline backup, go to step 6. To view and change the interruption settings, use the `ndmpfsconfig` command.

3. Stop the NFS, CIFS, FTP, SFTP, and TFTP services.
4. Use the `cifsbackup` command or the `nfsbackup` command to back up the file share information, as necessary.
For details about how to back up file share information, see the *CLI Administrator's Guide*.
5. Unmount and then remount the file system.
6. Verify that the file system that you want to back up is mounted, and if not, mount it.
7. Restart the NDMP server if you performed any of the following operations after the last restart:
 - Set or change the IP address or subnet mask of the node
 - Set or change the IP address or host name of the gateway
 - Add or change backup server information in the `/etc/hosts` file
8. Verify that the NDMP server is running normally.
9. Record the file system attributes such as the ACL type and the permissions and ACLs of all the directories above and for the directory used as the base point for the backup.
10. Use backup management software to perform the backup operation.
11. If you stopped the NFS, CIFS, FTP, SFTP, and TFTP services in step 3, start the services.

Restoring data from a tape device

This section explains how to restore data from a tape device.

When restoring files by specifying each file, if you specify more than 10,000 directories and files individually as restoration targets, restoration processing might end with an error. Make sure that the total number of directories and files does not exceed 10,000 by reducing the number of directories and files or by batch restoration of the data.

Before restoring data from backup media, use the `arcrestore` command to restore the HCP system data.

To restore data from a tape device

1. Set up the operating environment for the backup management software.
For details on how to set up the operating environment for the backup management software, see Backup Restore, supplementary material provided with the HDI system.
2. Prepare the restore-destination file system.
For the restore-destination file system, specify a capacity that is 105% or more of the size of the restore data and use the same ACL type as the one used when the data has been backed up. If you need to restore backup data of the Classic ACL type to a file system of the Advanced ACL type, you must take into account the amount of space required for ACL conversion. For details about migrating to a file system that uses the Advanced ACL type, see the *Installation and Configuration Guide*.
If you want to restore the data of the WORM file system, and the original file system can be used normally, restore the data to the original file system.
The data of a file system that supported 64-bit inodes needs to be restored in a file system that supports 64-bit inodes. If you restore the data in a file system that does not support 64-bit inodes, the number of files might exceed the maximum number of files that can be created in a file system.
To restore data to a file system that is different from the backup source, create a new file system. If you restore data in an existing file system, the number of files might exceed the maximum number of files that can be created in a file system.
3. Prepare the restore-destination directory.
Create the same directory hierarchy from the mount point to the parent directory of the restoration target, and set the same permissions for all the directories in the hierarchy as in the backup data. If the same directory hierarchy does not exist, directories from the mount point to the parent directory will automatically be created during the restore operation but might be assigned different permissions or ACLs from those present when a backup is performed.
To restore data to a WORM file system, the structure of the directories and files in the file system must be the same as when the data was backed up.

If you created a new file system, go to step 5.

4. Stop the NFS, CIFS, FTP, SFTP, and TFTP services, on the node that contains the file systems of the restore destination.
5. Verify that the file system that you want to back up is mounted with the read and write permissions enabled.
If not mounted, mount it in that manner.
6. Restart the NDMP server if you performed any of the following operations after the last restart:
 - Set or change the IP address or subnet mask of the node
 - Set or change the IP address or host name of the gateway
 - Add or change backup server information in the `/etc/hosts` file
7. Use backup management software to perform the restore operation.
If data for multiple file systems exists in the data to be restored, restore the data for each file system. If multiple directories and files with the same relative paths exist within the selected data, the data might be restored to an unintended state.



Note: When the restore operation is performed for a file or directory without using the DAR function, the processing time increases depending on the amount of backup data, not depending on the amount of data to be restored.

8. If you stopped the NFS, CIFS, FTP, SFTP, and TFTP services in step 4, start the services.
9. Create a file share on the file system.

Backing up system configuration

This chapter explains how to back up the system configuration.

- [Manually backing up the system configuration](#)
- [Regularly backing up system configuration](#)


Manually backing up the system configuration

This section explains how to manually back up the system configuration within the system and download the system configuration file to a disk outside of the system.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Save System Settings Menu page on page C-98](#)
- [Save All System Settings page on page C-98](#)

To manually back up the system configuration

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Backup Configuration** in the **Settings** area.
4. On the **Save System Settings Menu** page of the **Backup Configuration** dialog box, click **Save All System Settings**.
5. On the **Save All System Settings** page, click **Download**.
6. Click **OK**.


Regularly backing up system configuration

This section explains how to regularly (automatically) back up system configuration.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Save System Settings Menu page on page C-98](#)
- [Save All System Settings page on page C-98](#)
- [Schedule Settings for Saving All System Settings page on page C-100](#)
- [List of Mounted File Systems page on page C-102](#)

To regularly back up system configuration

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Backup Configuration** in the **Settings** area.

4. On the **Save System Settings Menu** page of the **Backup Configuration** dialog box, click **Save All System Settings**.
5. On the **Save All System Settings** page, click **Modify Schedule**.
6. On the **Schedule Settings for Saving All System Settings** page, specify the backup interval, backup time, and output setting. Select **Transfer to HCP**, **Output directory**, **Output to home directory**, or **Transfer to FTP server** for the output setting. If you select **Output directory**, click **Select**, select the file system to which you want to back up the system configuration file on the **List of Mounted File Systems** page, and then click **OK**.
7. Click **OK**.

Changing the network configuration

This chapter describes how to change the network configuration.

To change the data port setting, perform the necessary operations on the management console connected to the management port (`mng0`).

Note: If there are any errors in the network settings of the management port (`mng0`), you cannot connect to the HDI system from the management console, and as a result, you will experience difficulties in system recovery as a system administrator. Therefore, make sure there are no errors in the network settings after you have changed them.

- [Changing the IP address of a node](#)
- [Changing the host name of a node](#)
- [Adding and deleting routing information](#)
- [Changing the negotiation mode](#)
- [Setting up redundant link configuration](#)
- [Setting up a VLAN](#)


Changing the IP address of a node

This section explains how to change the IP address of a node.

GUI used for this operation

- [System Configuration Wizard on page C-23](#)
- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)
- [List of Interfaces page on page C-114](#)
- [Edit Interface page on page C-115](#)

To change the IP address of a node

1. In the top-left corner of the GUI, select **Action**, choose **Configuration Wizards**, and then **System Configuration Wizard**, to change the IP address of the `mng0` interface.
To change the IP address of an interface other than the `mng0` interface, go to step 8.
2. Click **Next** to display the **3. Basic Settings** page.
3. Click the **IPv4** tab and then change the IP address.
4. If you want to use IPv6, click the **IPv6** tab, and then change the IP address.
5. Click **Next**.
6. Verify the information displayed in the confirmation dialog box, and then click **Apply**.
7. Make sure that the processing results are correct, and then click **Finish**.
8. In the **System Information** panel, click .
9. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
10. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
11. On the **System Setup Menu** page (**Setting Type**: `network`), click **Interface Management**.
12. On the **List of Interfaces** page, select the protocol version for which you want to edit the information from the **Protocol version** drop-down list, and then click **Display**.
13. Select the interface with which the IP address is changed, and click **Edit**.
14. On the **Edit Interface** page, change the IP address, and click **OK**.
15. Change the physical network configuration as required.



Changing the host name of a node

This section explains how to change the host name of a node.

GUI used for this operation

- [System Configuration Wizard on page C-23](#)
- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Save System Settings Menu page on page C-98](#)
- [Save All System Settings page on page C-98](#)

To change the host name of a node

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Backup Configuration** in the **Settings** area.
4. On the **Save System Settings Menu** page of the **Backup Configuration** dialog box, click **Save All System Settings**.
5. On the **Save All System Settings** page, click **Download**.
6. When the download confirmation dialog box opens, click **OK**, and download the system settings file to storage media outside the system.
7. In the top-left corner of the GUI, select **Action**, choose **Configuration Wizards**, and then **System Configuration Wizard**.
8. Click **Next** to display the **3. Basic Settings** page.
9. Change the host name.
10. Click **Next**.
11. Verify the information displayed in the confirmation dialog box, and then click **Apply**.
12. Make sure that the processing results are correct, and then click **Finish**.
13. In the top-left corner of the GUI, choose the **Dashboard** tab, and then click **Refresh**.
The new host name is displayed in the **System Information** panel.
14. In the **System Information** panel, click .
15. In the *host-name* window, click **Backup Configuration** in the **Settings** area.
16. On the **Save System Settings Menu** page of the **Backup Configuration** dialog box, click **Save All System Settings**.
17. On the **Save All System Settings** page, click **Download**.
18. When the download confirmation dialog box opens, click **OK**, and download the system settings file to storage media outside the system.

Adding and deleting routing information


This section explains how to add and delete routing information.

Adding routing information

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)
- [List of Routings page on page C-119](#)
- [Add Routing page on page C-120](#)

To add routing information

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
5. On the **System Setup Menu** page (**Setting Type**: *network*), click **Routing Setup**.
6. On the **List of Routings** page, select the protocol version for which you want to add the information from the **Protocol version** drop-down list, and then click **Display**.
7. Click **Add**.
8. On the **Add Routing** page, enter the required information, and then click **OK**.

Deleting routing information


If the host name specified for the routing target or gateway cannot be resolved, you might not be able to delete the routing information correctly. If a host name is specified for the routing target or gateway, make sure that the host name can be resolved before you delete routing information.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)

- [List of Routings page on page C-119](#)

To delete routing information

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
5. On the **System Setup Menu** page (**Setting Type**: *network*), click **Routing Setup**.
6. Select the protocol version for which you want to delete the information from the **Protocol version** drop-down list, and then click **Display**.
7. Select the routing information you want to delete, and then click **Delete**.
8. Click **OK**.

If the *mng0* routing information is deleted, the dialog box might not be able to be opened from the **Settings** area in the *host-name* window. Log on to the GUI from other management console on the same network as the node, and set up the necessary routing information.

Changing the negotiation mode

This section explains how to change the negotiation mode of network ports.

If cascaded trunking is not set up for the port, see [Changing the negotiation mode \(for a non-cascaded trunk port\) on page 9-5](#). If it is set up for the port, see [Changing the negotiation mode \(for a cascaded trunk port\) on page 9-6](#).


Changing the negotiation mode (for a non-cascaded trunk port)

This section describes how to change the negotiation mode of a non-cascaded trunk port.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)
- [List of Data Ports page on page C-105](#)
- [Negotiation Mode Setup page on page C-107](#)

To change the negotiation mode of a non-cascaded trunk port

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
5. In the **System Setup Menu** page (**Setting Type**: *network*), click **Data Port Setup**.
6. In the **List of Data Ports** page, select the port to change the negotiation mode, and then click **Negotiation Mode Setup**.
If link alternation is set up for the port, make sure beforehand that the port is in *standby* status. The status of a link alternation port can be confirmed on the **List of Trunking Configurations** page (see [List of Trunking Configurations page on page C-111](#)).
7. In the **Negotiation Mode Setup** page, change the negotiation mode, and then click **OK**.
After changing the setting on HDI, reconfigure the connected switch accordingly.



Note: When the connected switch is reconfigured, the port might temporarily link down with the KAQG01013-W message.

8. In the **List of Data Ports** page, confirm that the negotiation mode has been changed.
9. If trunking is set on the port where you changed the negotiation mode, repeat steps 6 through 8 so that all ports included in the trunking are set to the same negotiation mode.
If link alternation is set, change the negotiation mode, wait 10 seconds, alternate the link manually, and then repeat steps 6 through 8. For information about how to perform manual link alternation, see [Performing manual link alternation on page 9-10](#).


Changing the negotiation mode (for a cascaded trunk port)

This section describes how to change the negotiation mode of a cascaded trunk port.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)
- [List of Data Ports page on page C-105](#)
- [Negotiation Mode Setup page on page C-107](#)

To change the negotiation mode of a cascaded trunk port

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
5. In the **System Setup Menu** page (**Setting Type**: *network*), click **Data Port Setup**.
6. In the **List of Data Ports** page, select a port of the link aggregation that is in *Standby* status, and then click **Negotiation Mode Setup**.
The status of a link alternation port can be confirmed on the **List of Trunking Configurations** page (see [List of Trunking Configurations page on page C-111](#)).
7. In the **Negotiation Mode Setup** page, change the negotiation mode, and then click **OK**.
After changing the setting on HDI, reconfigure the connected switch accordingly.



Note: When the connected switch is reconfigured, the port might temporarily link down with the KAQG01013-W message.

8. In the **List of Data Ports** page, confirm that the negotiation mode has been changed.
9. Repeat steps 6 to 8 so that all ports of the link aggregation that is in *Standby* status have the same negotiation mode.
10. After changing the negotiation mode, wait 10 seconds or so, and then perform manual link alternation.
For information about how to perform manual link alternation, see [Performing manual link alternation on page 9-10](#).
11. Repeat steps 6 to 9 for each port of the link aggregation that is now in *Standby* status.

Setting up redundant link configuration

This section explains how set up redundant link configuration.


Setting link aggregation

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)

- [System Setup Menu page on page C-103](#)
- [Link Aggregation Setup page on page C-113](#)

To set link aggregation

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
5. On the **System Setup Menu** page (**Setting Type**: *network*), click **Trunking Setup**.
6. On the **List of Trunking Configurations** page, select the ports for which you want to set link aggregation, and then click **Create Link Aggregation**.
7. On the **Link Aggregation Setup** page, click **OK**.
8. Click **OK**.
After setting the link aggregation, modify the settings of the destination switch.




Note: From the **Add Interface** page of the **Network & System Configuration** dialog box, you must add interfaces for the ports for which link aggregation is set ([Add Interface page on page C-116](#)).

Setting link alternation

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)
- [Link Alternation Setup page on page C-114](#)

To set link alternation

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.

5. On the **System Setup Menu** page (**Setting Type:** *network*), click **Trunking Setup**.
6. On the **List of Trunking Configurations** page, select two ports for which you want to set link alternation, and then click **Create Link Alternation**.
7. On the **Link Alternation Setup** page, select the default active port, and then click **OK**.
8. Click **OK**.
After setting the link alternation, modify the settings of the destination switch.




Note: From the **Add Interface** page of the **Network & System Configuration** dialog box, you must add interfaces for the ports for which link alternation is set ([Add Interface page on page C-116](#)).

Combining link aggregation and link alternation (cascaded trunking)

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)
- [List of Trunking Configurations page on page C-111](#)
- [Link Aggregation Setup page on page C-113](#)
- [Link Alternation Setup page on page C-114](#)

To combine link aggregation and link alternation

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
5. On the **System Setup Menu** page (**Setting Type:** *network*), click **Trunking Setup**.
6. On the **List of Trunking Configurations** page, select the ports for which you want to set link aggregation, and then click **Create Link Aggregation**.
7. On the **Link Aggregation Setup** page, click **OK**.
8. Click **OK**.

9. On the **List of Trunking Configurations** page, select two ports for which you want to set link alternation, including a link aggregation port. Then, click **Create Link Alternation**.
10. On the **Link Alternation Setup** page, select the default active port, and then click **OK**.
11. Click **OK**.
After setting the cascaded trunking, modify the settings of the destination switch.




Note: If cascaded trunking is enabled for a port, always set up a tagged VLAN for that port in order to stabilize the communication between the client and the HDI system. For details about how to setup a VLAN, see [Setting up a VLAN on page 9-10](#).

Performing manual link alternation

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)
- [List of Trunking Configurations page on page C-111](#)

To perform manual link alternation

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
5. On the **System Setup Menu** page (**Setting Type**: *network*), click **Trunking Setup**.
6. On the **List of Trunking Configurations** page, select a link alternation port, and then click **Change Active Port Status**.
7. Click **OK**.


Setting up a VLAN

To use a VLAN in an HDI system, a switch supporting an IEEE802.1Q tagged VLAN is required. When a VLAN is used, a virtual interface (a VLAN interface) is created for the data port. An identifier called a VLAN ID must be assigned to the VLAN interface.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [Network & System Configuration dialog box on page C-103](#)
- [System Setup Menu page on page C-103](#)
- [List of Interfaces page on page C-114](#)
- [Add Interface page on page C-116](#)
- [List of Routings page on page C-119](#)
- [Add Routing page on page C-120](#)

To set up a VLAN

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **network** from the **Setting Type** drop-down list, and then click **Display**.
5. On the **System Setup Menu** page (**Setting Type**: *network*), click **Interface Management**.
6. On the **List of Interfaces** page, select the protocol version for which you want to set the information from the **Protocol version** drop-down list, and then click **Display**.
7. Click **Add**.
8. On the **Add Interface** page, select a port that uses VLAN, specify a VLAN ID from 1 to 4094, specify other information, and then click **OK**.
9. On the **System Setup Menu** page (**Setting Type**: *network*), click **Routing Setup**.
10. On the **List of Routings** page, select the protocol version for which you want to add the information from the **Protocol version** drop-down list, and then click **Display**.
11. Click **Add**.
12. On the **Add Routing** page, select the port and VLAN ID, specify other information, and then click **OK**.

Monitoring the system

This chapter describes how to use SNMP or email notifications to monitor the system.

For details on the characters and settings that can be used for an SNMP manager, see the documentation of the SNMP manager.

- [Using SNMP](#)
- [Using error email notifications](#)

Using SNMP

By using SNMP, you can send SNMP trap notifications and obtain system operating information.

This section explains how to use SNMP.



Note:


- When using SNMP trap notifications, we recommend that you set the time of the SNMP manager to that of the OS. The SNMP manager clock is used to determine the SNMP trap reception time.
- If specific-trap settings for the HDI system are specified in the SNMP manager, you can limit the SNMP traps to be reported. For details about specific-trap settings, see the *Installation and Configuration Guide*.
- Some characters or settings described in this manual might be unusable depending on the SNMP manager you are using. For details about the characters and settings that can be used for an SNMP manager, see the documentation of the SNMP manager.
- To obtain system operating information when you are using SNMPv2 in an IPv4 environment, you need to specify the necessary settings on the **Add SNMP** or **Edit SNMP** page.
- To obtain system operating information or to use SNMP trap notifications when you are using SNMPv2 in an IPv6 environment or SNMPv3, you must edit the `snmpd.conf` file in the **Edit System File** page.
- Note the following regarding the editing of the `snmpd.conf` file:
 - To stop error notifications, change each line in the `snmpd.conf` file to a comment line by adding a hash mark (#) to the beginning of the line.
 - If the `com2sec6` setting specified in the `snmpd.conf` file is removed or changed to a comment, the initial `com2sec6` setting will be added when you perform an update installation. Revise the setting if necessary.

Using SNMPv2 in an IPv4 environment

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [System Setup Menu page on page C-103](#)
- [Edit System File page on page C-126](#)

To use SNMPv2 in an IPv4 environment

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.


4. In the **Network & System Configuration** dialog box, select **system** from the **Setting Type** drop-down list, and then click **Display**.
To only use the SNMP trap notification without obtaining system operating information, go to step 9.
5. On the **System Setup Menu** page (**Setting Type**: `system`), click **SNMP Setup**.
6. On the **List of SNMPs** page, click **Add**.
7. On the **Add SNMP** page, enter the required information, and then click **Add**.
8. On the **List of SNMPs** page, click **Back**
9. On the **System Setup Menu** page (**Setting Type**: `system`), click **Edit System File**.
10. On the **Edit System File** page, from the **File type** drop-down list, select the `snmpd.conf` file, and then click **Display**.
In the `snmpd.conf` file, add the setting required to enable SNMP trap notification. For details about the setting, see [Table C-113 Items displayed on the Edit System File page on page C-127](#).
11. Click **OK**.
12. Confirm that the `cold start` trap is issued.
If the trap is not issued, check the contents of the `snmpd.conf` file.

Using SNMPv2 in an IPv6 environment or SNMPv3

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [System Setup Menu page on page C-103](#)
- [Edit System File page on page C-126](#)

To use SNMPv2 in an IPv6 environment or SNMPv3

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **system** from the **Setting Type** drop-down list, and then click **Display**.
5. On the **System Setup Menu** page (**Setting Type**: `system`), click **Edit System File**.
6. On the **Edit System File** page, from the **File type** drop-down list, select the `snmpd.conf` file, and then click **Display**.

To use SNMPv3, add or edit the SNMP management user information, information for enabling SNMP trap notifications, and information for obtaining system operating information. For details about the setting, see [Table C-113 Items displayed on the Edit System File page on page C-127](#).

To use SNMPv2, add or edit the information about the SNMP manager permitted for access and the MIB objects that can be obtained.

7. Click **OK**.
8. Confirm that the `cold start` trap is issued after the `snmpd.conf` file is updated.
If the trap is not issued, check the contents of the file.

Table 10-1 Information specified in the `snmpd.conf` file when SNMPv3 is used

Configuration type	Configuration item	Description
<code>rouser</code> or <code>rwuser#</code>	User name	Specify a user name using no more than 32 characters. You can specify ASCII alphanumeric characters and the following ASCII symbols: <code># % - . : = _</code> A hash mark (#) cannot be used for the first character of a user name.
	Security level	Specify the security level for communication. <code>noauth</code> : Authentication is not used. <code>auth</code> : Authentication is used but encryption is not used. <code>priv</code> : Authentication and encryption are used. This item can be omitted.
	OID	When the security level is specified, specify the object ID that can be accessed by the user. This item can be omitted.
<code>createUser</code>	User name	Specify the user name that is used for SNMP communication. Use the user name specified for <code>rouser</code> or <code>rwuser</code> .
	Authentication type	If you specify <code>auth</code> or <code>priv</code> for the security level for <code>rouser</code> or <code>rwuser</code> , specify the type of user authentication. <code>MD5</code> : The HMAC-MD5-96 hash function is used. <code>SHA</code> : The HMAC-SHA1-96 hash function is used.
	Authentication password	When you specify an authentication type, specify an authentication password using at least 8 characters. You can specify ASCII alphanumeric characters and the following ASCII symbols: <code># % + - . / : = @ _</code>

Configuration type	Configuration item	Description
		A hash mark (#) cannot be used for the first character of an authentication password.
	Encryption type	If you specify <code>priv</code> for the security level for <code>rouser</code> or <code>rwuser</code> , specify the encryption type for the common key. DES: CBC-DES is used. AES: CFB-AES-128 is used.
	Encryption password	When you specify an encryption type, specify a password required for encryption by using at least 8 characters. You can specify ASCII alphanumeric characters and the following ASCII symbols: # % + - . / : = @ _ A hash mark (#) cannot be used for the first character of a password for encryption.
<code>trapsess -v3</code>	<code>-u</code> User name	Specify the user name that is used for trap notification. Use the user name specified for <code>rouser</code> or <code>rwuser</code> .
	<code>-l</code> Security level	If you specify the security level for <code>rouser</code> or <code>rwuser</code> , specify the same security level here. However, the specified strings are different from the ones specified for <code>rouser</code> or <code>rwuser</code> . <code>noAuthNoPriv</code> : Authentication is not used. <code>authNoPriv</code> : Authentication is used but encryption is not used. <code>authPriv</code> : Authentication and encryption are used.
	<code>-a</code> Authentication type	If you specify the authentication type for <code>createUser</code> , specify the same authentication type (MD5 or SHA).
	<code>-A</code> Authentication password	Specify the authentication password that is specified for <code>createUser</code> .
	<code>-x</code> Encryption type	If you specify the encryption type for <code>createUser</code> , specify the same encryption type (DES or AES).
	<code>-X</code> Encryption password	Specify the password for encryption that is specified for <code>createUser</code> .
	Host name or IP address of the SNMP manager	Specify the host name or IP address of the SNMP manager to which trap notification is sent.
	Port number	Specify the port number that is used for trap notification in the following format: <i>SNMP-manager-host-name-or-IP-address:port-number</i> You can skip this setting for SNMP manager using IPv4. If you skip this setting, the allocated port number is 162.

Configuration type	Configuration item	Description
		You cannot skip this setting for SNMP manager using IPv6.
		#: <code>rwuser</code> is the setting when reading and writing of a MIB object are permitted; however, HDI does not support writing to MIB objects.


Using error email notifications

This section explains how to use email for the notification of error information.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [System Setup Menu page on page C-103](#)
- [Edit System File page on page C-126](#)

To use email notifications

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Network & System Configuration** in the **Settings** area.
4. In the **Network & System Configuration** dialog box, select **system** from the **Setting Type** drop-down list, and then click **Display**.
5. On the **System Setup Menu** page (**Setting Type**: `system`), click **Edit System File**.
6. On the **Edit System File** page, from the **File type** drop-down list, select the `email_alert.conf` file, and then click **Display**.
7. Append the mail server information and the recipient and sender email addresses to this file.
8. Click **OK**.
9. Confirm that the test email is received.

A test email is sent with the title `HDI Alert (node-host-name KAQM09112-I)`.

If you do not receive the test email within five minutes after clicking **OK** at the specified recipient email address, verify the following and take action as appropriate:

- The definitions in the `email_alert.conf` file are valid.
- The mail server settings are correct.

- The system message KAQM09113-E is not output to the **List of RAS Information** page (for List of messages) (see [List of RAS Information page on page C-39](#)).

Error information emails are sent with the title `HDI Alert (node-host-name message-ID)`.



Note: If you are unable to receive error email notifications after enabling them, verify the following and take action as appropriate:

- The system messages KAQM09113-E, KAQM09114-E, KAQM09115-E, KAQM09116-E, and KAQM09117-E are not output to the **List of RAS Information** page (for List of messages) (see [List of RAS Information page on page C-39](#)).
 - The definitions in the `email_alert.conf` file are valid.
 - The mail server settings have not changed.
-



Tip: To stop error notifications, place a hash mark (#) at the beginning of each entry line in the `email_alert.conf` file.

Setting up an environment for command and GUI operations

This chapter describes how to set up an environment for command and GUI operations.

- [Setting up the SSH environment to use commands](#)
- [Setting up a public key certificate](#)

Setting up the SSH environment to use commands

This section explains how to register a public key to use commands.


Prerequisites for registering a public key

SSH2 is supported in HDI systems. Use a key creation tool to create the private key and public key that are used in the SSH authentication. Create the public key in OpenSSH format. For details about how to install the relevant software and create those keys, see the documentation provided with the software. The passphrase specified when creating the keys is used as the SSH log on password. You can omit a passphrase.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [List of Services page on page C-137](#)
- [Public Key List page on page C-176](#)
- [Add Public Key page on page C-176](#)

To register a public key to use commands

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Access Protocol Configuration** in the **Settings** area.
4. On the **List of Services** page of the **Access Protocol Configuration** dialog box, select **SSH**, and then click **Modify Configuration**.
5. On the **Public Key List** page, click **Add**.
6. On the **Add Public Key** page, specify the public key file, and then click **Add**.

The public key is registered for the SSH account `nasroot`.

For details about how to use commands, see the *CLI Administrator's Guide*.

Setting up a public key certificate

This section describes how to set up a public key certificate issued by a certification authority (CA) for a node.

A self-signed certificate has been set up in the node using the default setting because communication between a node and GUI is based on SSL. To use a public key certificate issued by a certificate authority, obtain a certificate from a certificate authority and set the certificate up for a node.

Public key certificates and intermediate certificate authority certificates can be set for a node. Cross certificates cannot be applied.

The execution of commands is required for this operation. See [Setting up the SSH environment to use commands on page 11-2](#) to set up a proper environment. For details about how to use commands, see the *CLI Administrator's Guide*.

To set up a public key certificate issued by a certificate authority for a node

1. Execute the `certctl` command by using the `--create-cert` option to create a certificate signing request (CSR) and private key.

```
certctl --create-cert --dest-key private-key-file-name --dest-csr CSR-file-name --key-passwd private-key-password [--country country-name] [--state-province state-or-province-name] [--locality locality-name] [--organization company-or-organization-name] [--unit organization-or-department-unit-name] [--common-name host-name-of-node] [--email E-mail-address]
```

The certificate signing request and private key file will be output to the SSH account home directory (`/home/nasroot`).

2. Use the `scp` command or any other method to transfer the CSR file to the local disk of the management console or any other appropriate location.
3. Send the certificate signing request to a certificate authority to obtain a public key certificate.
4. Use the `scp` command or any other method to transfer the public key certificate file obtained from the certificate authority to the HDI. Transfer the file to the home directory for the SSH account (`/home/nasroot`).
5. Execute the `certctl` command by using the `--create-pkcs` option to create a keystore in PKCS #12 format.

```
certctl --create-pkcs --key private-key-file-name --cert public-key-certificate-file-name [--intermediate-cert intermediate-certificate-authority-certificate-file-name] --dest-keystore keystore-file-name --passwd keystore-password --key-passwd private-key-password
```

The keystore file in PKCS #12 format will be output to the SSH account home directory (`/home/nasroot`).

6. Use the `scp` command or any other method to transfer the keystore file in PKCS #12 format to the local disk of a machine that has Oracle JDK 6 or later installed.
7. Import the keystore in PKCS #12 format to a keystore in JKS format. To do this, the machine you are using must have Oracle JDK6 or later installed.

Here is an example of creating a keystore file on a Windows machine.

```
keytool.exe -alias certificate -importkeystore -srckeystore path-of-keystore-in-PKCS-#12-format -destkeystore path-of-keystore-in-JKS-format -
```

```
srcstoretype pkcs12 -deststoretype jks -destalias alias-name-of-your-choice -destkeypass changeit
```

If you are prompted to enter the password for the destination keystore, enter the `changeit`. If you are prompted to enter a password for the source keystore, enter the password that you specified when you created the keystore in PKCS #12 format.

8. Use the `scp` command or any other method to transfer the keystore file in JKS format to the HDI.

Transfer the file to the home directory for the SSH account (`/home/nasroot`).

9. Execute the `certctl` command by using the `--set-cert` option to set up the following for the node: the certificate obtained from the certificate authority, the created private key, and the keystore in JKS format.

```
certctl --set-cert --key private-key-file-name --cert public-key-certificate-file-name [--intermediate-cert intermediate-certificate-authority-certificate-file-name] --keystore keystore-file-name --key-passwd private-key-password [-y]
```



Tip: To initialize the setting of a public key certificate set up in a node, execute the `certctl` command by using the `--reset` option.

Performing an update installation

This chapter describes how to perform an update installation for software.

- [Updating software](#)

Updating software

This section explains how to update software running on a node. To update by using the installation file registered in an HCP system, see [Updating software \(using the installation file registered in an HCP system\) on page 12-2](#). To update by using the installation media, see [Updating software \(using an installation media\) on page 12-3](#).

Notes:

- If you update the software in an environment where the OS or web browser of the management console is not configured to support SHA-2, you will no longer be able to communicate with the node. Ensure that the OS or web browser is configured to support SHA-2 before you update the software.
- You cannot use the GUI or a command to execute other operations during a software update.
- Performing an upgrade installation will disable communication with the current node if you specify a password of 65 or more characters as the secret key for the public key certificate by using the `certctl` command with the `--key-passwd` option. If the password of 65 or more characters has been set, reset the certificate settings by executing the `certctl` command with the `--reset` option specified, and then perform the upgrade installation.



Note: Security enhancement is disabled initially when the HDI system is upgraded from a version other than 5.4.1-xx, 6.1.1-xx, 6.1.2-xx, 6.2.x-xx, 6.3.x-xx, or 6.4.x-xx (regardless of the number of x). You can use the `secureshellctl` command to enable security enhancement. For details about the `secureshellctl` command, see the *CLI Administrator's Guide*.

If you want to enable security enhancement, note the following points:

- If you enable security enhancement, you will not be able to disable it.
 - The following operations, which are not supported by the HDI system, are restricted:
 - Executing LINUX commands
 - Executing scripts in the HDI system
 - Redirecting command output to a file
-

Updating software (using the installation file registered in an HCP system)


This subsection explains how to use the installation file registered in an HCP system to update the software running on a node.

GUI used for this operation

- [System Information panel on page C-46](#)
- [host-name window on page C-51](#)
- [System Software Installation dialog box on page C-85](#)

- [Save System Settings Menu page on page C-98](#)
- [Save All System Settings page on page C-98](#)

To update the software running on a node by using the installation file registered in an HCP system:

1. In the top-left corner of the GUI, choose the **Dashboard** tab.
2. In the **System Information** panel, click .
3. From the *host-name* window, click **Software Update** in the **Settings** area.
4. If the HCP Anywhere is not linked, click **Backup Configuration** in the **System Software Installation** dialog box.
If the HCP Anywhere is linked, go to step 9.
5. On the **Save System Settings Menu** page of the **Backup Configuration** dialog box, click **Save All System Settings**.
6. On the **Save All System Settings** page, click **Download**.
7. If the information displayed in the confirmation dialog box is correct, click **OK**, and then download the system configuration file to a disk outside of the system.
8. On the **Save All System Settings** page, click **Close**.
9. In the **System Software Installation** dialog box, select the software version to be installed and the check box, and then click **Install**.

Updating software (using an installation media)

This subsection explains how to use an installation media to update the software running on a node.

Before updating the software on a node

- Download all the log files, core files, and dump files before performing the installation. After downloading the log files, core files, and dump files, delete the files on the HDI node.
- The node OS must be stopped. To stop the node OS, execute the `nasshutdown` command before performing the installation.
- Make sure that node services are stopped during installation.

To update the software running on a node by using an installation media:

1. Connect the devices (such as the keyboard and monitor) that were used when the system was first set up to the node.
2. Use the power switch or power button on the node to turn on the node.
For details about how to use the power switch or power button on the node, see [Starting and forcibly stopping a node OS on page H-2](#).

3. If `Press to enter setup` is displayed in the window, press the **Delete** key.
4. Select `Boot` from the Main Menu window.
5. Verify the information displayed in the Boot Menu window.

Verify that the items under `Boot Option Priorities` are displayed in the following order:

```

Boot Option Priorities
Boot Option #1           [xxxxxxxxxxxxxxxxxxxx#]
Boot Option #2           [(Bus xx Dev xx)PCI ...]
Boot Option #3           [Built-in EFI Shell]

```

If the displayed order is different from the order shown above, change the displayed order to the order shown above by selecting the item whose order you want to change, and then press the **Enter** key.

`#`: Information about the external DVD drive is displayed.

6. Insert the installation disc into the node's optical drive.
7. From the Boot Menu window, select `Save & Exit`.
8. From the Exit Menu window, select `Save Changes and Reset` if the settings were changed. From the Exit Menu window, select `Discard Changes and Exit` if the settings were not changed.

A confirmation message appears. Select `Yes`, and then press the **Enter** key. If you select `Save Changes and Reset`, the node restarts.

After then, the installation menu is displayed on the monitor that is connected to the node.

9. Enter `2` in the installation mode selection window.

```

[Select mode]
1. Initial install
2. Update install
3. Maintenance
KAQG61000-I Select a mode, and then press the [Enter] key. (1/2/3):2

```

10. Enter `y` in the backup confirmation window.

If the system settings were not saved before the start of the installation, enter `n` and take action according to the message to stop the installation.

```

[Install parameters]
The settings have not been saved. If there is no current settings file
before the update is installed, the system cannot be restored. Have you
acquired the settings file? (y/n):y

```

11. Enter `y` in the backup confirmation window.

If the system settings were not saved before the start of the installation, enter `n` and take action according to the message to stop the installation.

```

[Install parameters]
Check the acquired settings file. Was this file acquired during an update
installation? (y/n):y

```

12. Make sure that the information displayed in the installation confirmation window is correct, and then enter `y`.

Make sure that the product name and version displayed for Information on product to be installed are correct.

```
[Mode]
2. Update install

[Install parameters]
Installation model: Single

[Installed product information]
Product name           Version
Hitachi Data Ingestor 4.1.0-00

[Information on product to be installed]
Product name           Version
Hitachi Data Ingestor 4.1.2-00

KAQG61005-Q Are you sure you want to execute the selected mode? (update
install) (y/n):y
```

The installation progress window is displayed and the installation starts. After the installation completes, `Completed` is displayed for `Status`. If the installation fails, an error message appears. Contact maintenance personnel.

13. Check the information displayed in the installation complete window, take out the installation disc as instructed in the message, and then press the **Enter** key.

The node restarts. The **LILO Boot Menu** window might be displayed, interrupting the restarting of the node. If this happens, check the information displayed in the window, and then press the **Enter** key to restart the node again.

14. Confirm that the login window is displayed on the monitor that is connected to the node.

If the node is restarted and the login window is displayed on the monitor, the installation is complete.



Note: Make sure that the conditions below are satisfied after the installation is completed. If there are problems, see the *Single Node Troubleshooting Guide* and take the necessary measures.

- There are no problems with the FC paths when a storage system is connected to the node. (See [Hardware window on page C-72](#) or the description of the `fpstatus` command.)
- There are no problems with the status of the file system. (See [File Systems window on page C-56](#) or the description of the `fslist` command.)
- The system version is up-to-date. (See [host-name window on page C-51](#) or the description of the `versionlist` command.)
- The node is running normally. (See [host-name window on page C-51](#) or the description of the `rgstatus` command.)
- There are no problems with the hardware status of the node. (See [Hardware window on page C-72](#) or the description of the `hwstatus` command.)

If you are using a front bezel, carefully attach the front bezel according to the manual. If you do not know how to attach the front bezel, contact maintenance personnel.



A

Operations provided by the GUI

This appendix describes the operation of the GUI.

- [List of operations](#)

List of operations

The following operations can be performed using the GUI.

Table A-1 Operations provided by the GUI

Operation		See
Managing System Administrator Accounts	Changing the password of a system administrator	Change System Admin Password dialog box on page C-35
	Changing the account security settings	Login Security dialog box on page C-38
Managing a Node	Viewing the status of a node	host-name window on page C-51
	Changing the settings for a node	System Configuration Wizard on page C-23
	Restarting a node	Restart Node dialog box on page C-84
Managing HCPs	Setting HCP information	Service Configuration Wizard on page C-24
	Setting proxy server information	Configure Proxy Server dialog box on page C-34
Managing File Systems	Creating a file system	Create File System dialog box on page C-215
	Deleting a file system	Delete File System dialog box on page C-235
	Changing the settings for a file system	Edit File System dialog box on page C-228
Managing File Shares	Adding a file share	Add Share dialog box on page C-208
	Releasing a file share	Release Share(s) dialog box on page C-204
	Editing the attributes of a file share	Edit Share dialog box on page C-198
Managing Tasks	Managing migration tasks	Migration Tasks dialog box on page C-4
	Managing a task for importing files	Import Files window on page C-81
	Importing files	Import Files dialog box on page C-27
	Adding a cache resident policy	Add Cache Resident Policy dialog box on page C-237
	Editing a cache resident policy	Edit Cache Resident Policy dialog box on page C-237
	Deleting a cache resident policy	Delete Cache Resident Policy dialog box on page C-238

Operation		See
Managing Services	Controlling a service	Service Configuration Wizard on page C-24
	Changing the configuration definition of the NFS service	NFS Service Management page on page C-168
	Changing the configuration definition of the CIFS service	CIFS Service Management (Basic) page on page C-141
	Maintaining the CIFS service	CIFS Service Maintenance page on page C-177
	Changing the configuration definition of the SSH service	Public Key List page on page C-176
	Changing the configuration definition of the FTP service	FTP Service Management page on page C-162
	Changing the configuration definition of the SFTP service	SFTP Service Management page on page C-171
System Setup	Setting up ports	List of Data Ports page on page C-105
	Setting up and disabling trunking	List of Trunking Configurations page on page C-111
	Setting up an interface information	List of Interfaces page on page C-114
	Setting information for the DNS server, the NIS server, and the LDAP server for user authentication	DNS, NIS, LDAP Setup page on page C-117
	Setting routing information	List of Routings page on page C-119
	Specifying time-related settings	Time Setup page on page C-122
	Setting the destination for transferring system log data	Edit Syslog Setup page on page C-124
	Setting the log file size	Log File Capacity Setup page on page C-125
	Setting the data retention period for core files	Core File Auto. Deletion Setup page on page C-126
	Directly editing system files	Edit System File page on page C-126
	Tuning system performance	Performance Tuning page on page C-133
	Setting up SNMP	List of SNMPs page on page C-134
Managing Anti-Virus Functionality	Setting up scan software	Scanning software page on page C-196
	Registering a scan server	Add Scanner Server page on page C-189

Operation		See
	Changing the settings of a registered scan server	Edit Scanner Server page on page C-189
	Deleting a registered scan server	List of Scanner Servers page on page C-186
	Setting scan conditions	Scan Conditions page on page C-190
	Enabling or disabling real-time scanning	List of Scanner Servers page on page C-186
Managing Local Users and Groups	Managing local users	Local Users dialog box on page C-85
	Managing local groups	Local Users dialog box on page C-85
Viewing Hardware Information	Viewing hardware information	Hardware window on page C-72
Managing Software	Updating software installed on a node	System Software Installation dialog box on page C-85
Collecting System Configuration Information	Saving system settings	Save All System Settings page on page C-98
	Downloading system settings files	Save All System Settings page on page C-98
	Uploading system settings files	Upload Saved Data page on page C-102
	Setting periodic saving of the system settings	Schedule Settings for Saving All System Settings page on page C-100
Managing Node Error Information	Managing system messages	List of RAS Information page (for List of messages) on page C-40
	Managing system logs	List of RAS Information page (for List of system logs) on page C-41
	Managing other log files	List of RAS Information page (for List of other log files) on page C-42
	Downloading or deleting log files all at one time	List of RAS Information page (for Batch-download) on page C-42
	Managing core and dump files	List of RAS Information page (for List of core files) on page C-43
	Viewing the status of the connections with external servers	List of RAS Information page (for Server check) on page C-44
	Using SNMP to send error information	Edit System File page on page C-126
	Using email to send error information	Edit System File page on page C-126

Basic GUI operation

This appendix describes basic GUI operations.

- [Window configuration](#)
- [Notes on using the GUI](#)

Window configuration

The following figure shows the layout of the window after logging on to an HDI system via the GUI.

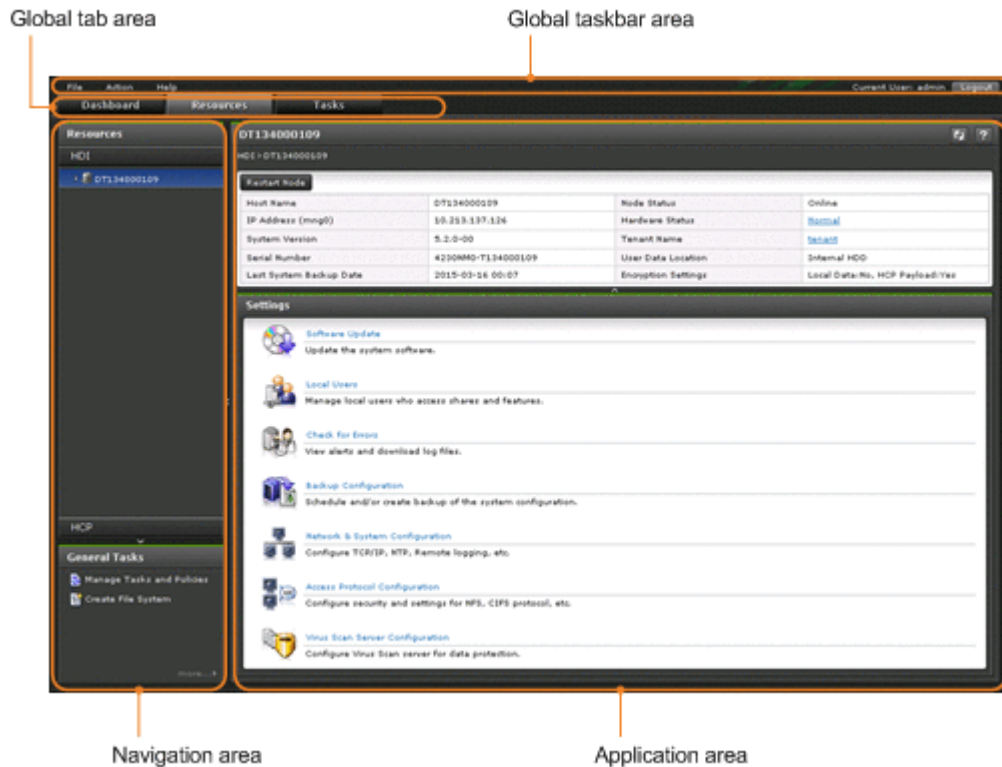


Figure B-1 Overview of the window layout

Global taskbar area

The global taskbar area is used to start system setup and to display help.

Table B-1 Items displayed in the global taskbar area

Item		Description
File	Logout	Logs out of an HDI system and terminates operation management.
Action	Manage Tasks and Policies Migration Tasks	Manages migration policy tasks (migration tasks). Manages migration tasks.
	Configuration Wizards	System Configuration Wizard Sets up the system. Service Configuration Wizard Sets up services.
	Chargeback Report	Acquires statistics related to the usage status of tenants.
	Import Files	Imports data from another file server.

Item	Description
Configure Proxy Server	Specifies information about the proxy server to be used for communication between nodes and HCP.
Change Password	<p>Change System Admin Password Changes the password for the HDI system administrator account.</p> <p>Change HCP Tenant Admin Password Changes the password for the HCP Tenant administrator.</p> <p>Update HCP Anywhere Credentials Changes the password to be used for accessing HCP Anywhere.</p>
Login Security	Changes the security settings for a system administrator account.
Download All Log Data	Downloads log files in a batch operation. In batch downloading, multiple log files are archived by <code>tar</code> and compressed by <code>gzip</code> .
Launch	<p>Check for Errors Checks the messages and logs output during operation of an HDI system.</p>
Help	Online Manual Displays a list of HDI online manuals.

Global tab area

The global tab area allows you to toggle between a window that gives an overview of the system status, and a window for checking system settings and status details.

Table B-2 Items displayed in the global tab area

Item	Description
Dashboard	Gives an overview of the system status.
Resources	File shares, file systems, volume groups, hardware, and the HCP system are managed.
Tasks	Allows you to manage tasks, such as migration and importation of files from another file server.

Navigation area

The navigation area allows the tree to be expanded to select objects whose settings and status are to be checked. This is displayed by selecting the **Resources** or **Tasks** tab in the global tab area.

Table B-3 Items displayed in the navigation area (when the Resources tab is selected in the global tab area)

Item		Description	
Resources	HDI	<i>host-name</i>	<p>Select this to check the HDI settings and statuses.</p> <p>Select the triangle icon on the left to display the following items:</p> <p>Shares</p> <p>Select this to check the list of file shares.</p> <p>File Systems</p> <p>Select this to check the list of file system statuses.</p> <p>Select the triangle icon on the left to display the name of the file system, which can be selected to check the status of the individual file system.</p> <p>Volume Groups</p> <p>Select this to check the list of volume group statuses.</p> <p>Hardware</p> <p>Select this to check the operating status of the system, and whether hardware is working properly.</p>
	HCP		Select this to check the status of settings related to HCP tenants and namespaces.
General Tasks	Manage Tasks and Policies		Select this to manage migration tasks.
	Create File System		Select this to create a file system.

Table B-4 Items displayed in the navigation area (when the Tasks tab is selected in the global tab area)





Item		Description
Tasks	Import Files	Select this to manage importation of files from another file server.
	Other Tasks	Select this to manage migration tasks.

Application area

The application area displays information about the object selected in the navigation area. In the application area, you can change the object settings and add or delete the objects.

- To select an object in the table:
 - Click the check box, radio button, or row. Click the row of the operation target to highlight the row. To select multiple objects, select

multiple check boxes, or click rows while pressing the **Ctrl** or **Shift** key.

- To change the column display order:
Drag and drop the table headers.
- To show and hide columns:
Click the **Column Settings** button to specify the names of the columns to be displayed. From the dialog box that is displayed when the **Column Settings** button is clicked, you can see item descriptions as well as drag and drop rows to change the display order.
- To sort the displayed items:
Click the table header to toggle between ascending and descending order.
- To filter displayed items:
Click the **Filter** button, and then specify conditions. Select either **On** or **Off** for the filtering option to hide or show the filtered display items.
- To display information page by page:
From the **Rows/page** drop-down list, select the number of lines to be displayed per page. In the **Page** text box, the page number of the currently displayed page and the total number of pages are displayed. You can move to the specified page by entering the page number in the text box and pressing the **Enter** key. You can also click buttons to display the first page, the previous page, the next page, or the final page.
- To update displayed information:
Click  (update).
- To get help:
Click  (help).
- To maximize or minimize a dialog box:
Click  (maximize) or  (minimize).

Notes on using the GUI

Note the following when using the GUI:

- Do not open multiple windows to perform operations simultaneously.
- Some time might be required to display recently updated information in the GUI.
- If a window is closed while a page is loading, an error sometimes occurs the next time a window is opened, and no operations can be performed. If this happens, close all open Web browsers, and then start over from the beginning.

- If you perform an operation in a dialog box while the network load is high, some information might not be displayed in the dialog box. If this happens, close and re-open the dialog box, confirm the status, and then perform the intended operation.
- If you have changed the linked HCP version, you also need to update information in the HDI database. After clicking the update button, log out from the system, and then log in again.

GUI reference

This appendix describes items displayed in the GUI and how to use each window.

- [Migration Tasks dialog box](#)
- [Download Report dialog box](#)
- [Failed dialog box](#)
- [Policy Information dialog box](#)
- [Migration Task Wizard](#)
- [File Systems dialog box](#)
- [Stop Task dialog box](#)
- [Migrate Immediately dialog box](#)
- [Enable Task dialog box](#)
- [Disable Task dialog box](#)
- [Delete Task dialog box](#)
- [System Configuration Wizard](#)
- [Service Configuration Wizard](#)
- [Download Chargeback Report dialog box](#)

- [Import Files dialog box](#)
- [Configure Proxy Server dialog box](#)
- [Change System Admin Password dialog box](#)
- [Change HCP Tenant Admin Password dialog box](#)
- [Update HCP Anywhere Credentials dialog box](#)
- [Login Security dialog box](#)
- [Check for Errors dialog box](#)
- [Dashboard tab](#)
- [host-name window](#)
- [Shares window](#)
- [File Systems window](#)
- [file-system-name window](#)
- [Volume Groups window](#)
- [Hardware window](#)
- [tenant-name window](#)
- [Import Files window](#)
- [Restart Node dialog box](#)
- [System Software Installation dialog box](#)
- [Local Users dialog box](#)
- [Backup Configuration dialog box](#)
- [Network & System Configuration dialog box](#)
- [Access Protocol Configuration dialog box](#)

- [Virus Scan Server Configuration dialog box](#)
- [CIFS Protocol Settings dialog box](#)
- [NFS Protocol Settings dialog box](#)
- [Edit Share dialog box](#)
- [Release Share\(s\) dialog box](#)
- [Edit CIFS Share Host or Network dialog box](#)
- [Add CIFS Share Host or Network dialog box](#)
- [Edit NFS Share Host or Network dialog box](#)
- [Add NFS Share Host or Network dialog box](#)
- [Add Share dialog box](#)
- [Create File System dialog box](#)
- [Edit File System dialog box](#)
- [Delete File System dialog box](#)
- [Advanced ACL Settings dialog box](#)
- [Add Cache Resident Policy dialog box](#)
- [Edit Cache Resident Policy dialog box](#)
- [Delete Cache Resident Policy dialog box](#)
- [Provisioning Wizard](#)

Migration Tasks dialog box

You can manage migration tasks as units for which migration is performed.

To display the **Migration Tasks** dialog box, from the **Action** menu in the top-left corner of the GUI, choose **Migration Tasks**.



Note:

- Do not change or delete the namespace set for a file system for which a migration has already been started. Changing or deleting the namespace for a file system that migrated files rely on might cause migrated files to become inaccessible or might cause subsequent migrations to fail.
- The `.arc` directory, which is used for storing management information, is created directly under a file system for which migration operations have started. Do not delete the `.arc` directory or any files under the directory. If the directory or any files under the directory are deleted, use the `arccorrection` command to restore them.
- Increasing the number of migration tasks to be executed concurrently puts a heavier load on the system. If too many migration tasks are executing concurrently, putting a heavy load on the system, adjust the schedule so that fewer migration tasks execute concurrently.
- Migration tasks cannot be set for file systems that reference other HDI data as read-only via the linked HCP. Furthermore, tasks other than the default migration tasks cannot be set for home-directory-roaming file systems or read-write-content-sharing file systems.



Tip: Task management information is recorded when a file is accessed or updated in a file system for which migration is set up. The task management information is used to determine whether files are migrated. If a failure occurs, or a migration task is set for a file system for which migration is set, the task management information is rebuilt. If a failure occurs or a migration task is set for a file system for which migration is currently being performed, processing to reconstruct the task management information is executed in the background. If this happens, set a migration task so that the migration is performed again, after the task management information has finished being rebuilt. In order to confirm whether task management information is being or has been rebuilt, check for the KAQM37137-I system message, which is output when rebuild processing starts, and the KAQM37139-I system message, which is output when rebuild processing finishes. For details about how to check system messages, see [List of RAS Information page on page C-39](#).

If a migration task is set up for the first time for a file system on which files have been created and the schedule is set up to perform only one migration, the migration might not be performed. If the migration was not performed, set up another migration task after the KAQM37139-I message has been output.

Some files might not be migrated depending on the status of the system during a migration. To ensure that all files are correctly migrated, set up a migration task schedule so that migrations are performed on a regular basis.

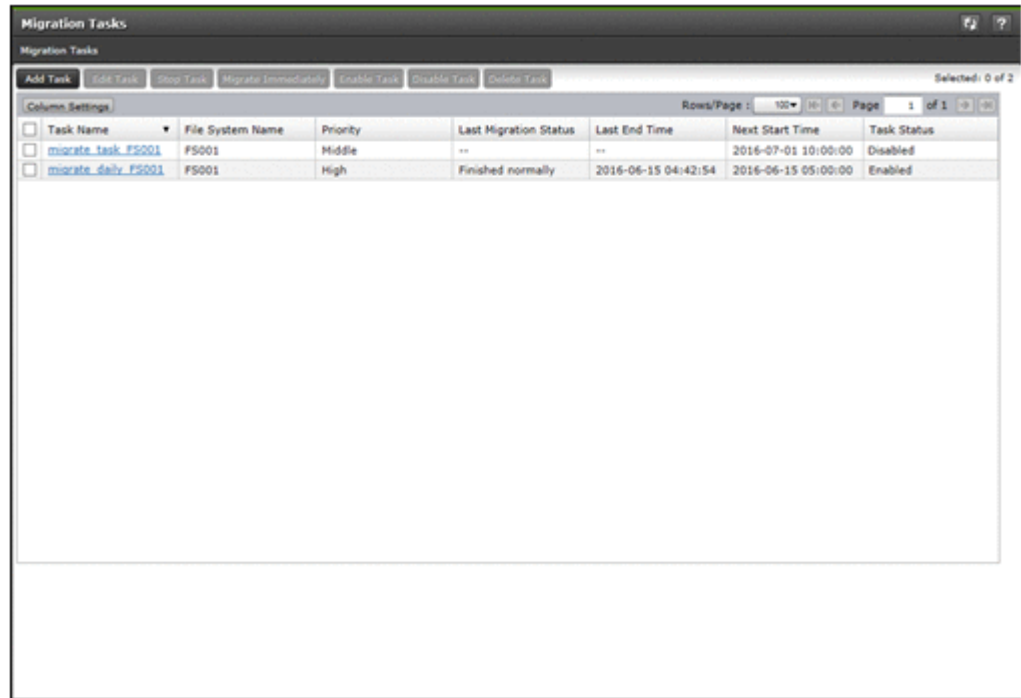






Table C-1 Items displayed on the Migration Tasks dialog box

Item	Description	See
Add Task button	Adds a migration task.	Migration Task Wizard on page C-15
Edit Task button	Allows the user to edit the settings of the selected migration task.	Migration Task Wizard on page C-15
Stop Task button	Stops the selected migration task.	Stop Task dialog box on page C-20
Migrate Immediately button	Immediately run the selected migration task.	Migrate Immediately dialog box on page C-20
Enable Task button	Enables the selected migration task.	Enable Task dialog box on page C-21
Disable Task button	Disables the selected migration task.	Disable Task dialog box on page C-21
Delete Task button	Deletes the selected migration task.	Delete Task dialog box on page C-22
Column Settings button	Sets the columns to be displayed. In the dialog box that appears when you click Column Settings , select the columns you want to	N/A

Item	Description	See
	display, and then click OK . Note that, if you click Restore Default Settings , all columns will be selected.	
Rows/Page	Select, from the drop-down list box, the maximum number of rows to be displayed on a page.	N/A
Page	When information is displayed on multiple pages, specify, in the text box, the page number of the page you want to view. Alternatively, click  or  to move to the previous or following page, respectively. Similarly, click  or  to move to the first or last page, respectively.	N/A
Task Name	The name of the migration task.	N/A
File System Name	The name of the file system corresponding to the migration task.	N/A
Priority	The priority level of the migration task to be executed according to a schedule. High The priority is High (1 to 3). Middle The priority is Middle (4 to 6). Low The priority is Low (7 to 10).	N/A
Last Migration Status	The status of the migration task that was last executed. Executing The task is executing. Finished normally The task that was last executed ended successfully. Partially failed Processing for the task that was last executed finished, but the migration of some files or directories failed. Use the Download Report dialog box or the <code>arcresultctl</code> command to check the message that was output when the migration failed, resolve the problem, and then execute the task again. Note that, when you execute the task again, files and directories that are not subject to the applicable policy will not be migrated. Failed to start (Message ID) An attempt to execute the task failed. Interrupted	N/A

Item	Description	See
	Task processing was interrupted because of one of the following reasons: a maximum duration, or interruption; or the file system was unmounted. If the task is interrupted repeatedly, change the maximum duration value. If no migration task was executed, -- is displayed.	
Last End Time	The date and time when the migration task that was last executed finished. If no migration task was executed, -- is displayed.	N/A
Next Start Time	The date and time when the next migration task is to be executed next time.	N/A
Task Status	Indicates whether a migration task is enabled. Enabled The migration task is enabled. Disabled The migration task is disabled.	N/A
Note: N/A = Not applicable.		

migration-task page

You can use this page to view detailed information about a specific migration task.

To open the *migration-task* page, click the desired *migration-task* link in the **Migration Tasks** dialog box.



Tip: To go back to the **Migration Tasks** dialog box, click the part **Migration Tasks** of **Migration Tasks** > *migration-task* at the top left of the window.

Table C-2 Items displayed on the migration-task page

Item	Description	See
Enable Task button	Enables the migration task.	N/A
Disable Task button	Disables the migration task.	N/A
Download Report button	Downloads a list of files and directories whose migration succeeded or failed (text file in UTF-8 format).	Download Report dialog box on page C-12
Task Name	The name of the migration task.	N/A
File System Name	The name of the file system.	N/A

Item	Description	See
Task Information	Information about the migration task.	Task Information tab on page C-8
	Task Details Detailed information about the migration task.	
	Policy Details Detailed information about the migration policy.	
History	The migration history.	History tab on page C-11
Note: N/A = Not applicable.		

Task Information tab

You can use the **Task Information** tab to view the information about the migration task.

Task Details subtab

You can use the **Task Details** subtab to view the detailed information about the migration task.

Table C-3 Items displayed on the Task Details subtab of the Task Information tab in the migration-task page

Item	Description
Execution ID	<p>The execution ID of the migration task. The format of the execution ID is as follows:</p> <p><i>date-in-YYYYMMDD-format-execution-serial-number-of-the-migration-task-in-NNN-format</i></p> <p>Note that, if the migration task is currently executing, the execution ID will not be displayed. Instead, -- will be displayed.</p>
Priority	<p>The priority level of the migration task to be executed according to a schedule.</p> <p>High The priority is High (1 to 3).</p> <p>Middle The priority is Middle (4 to 6).</p> <p>Low The priority is Low (7 to 10).</p>
Last Migration Status	<p>The status of the migration task that was last executed.</p> <p>Executing The task is executing.</p> <p>Finished normally The task that was last executed ended successfully.</p> <p>Partially failed</p>

Item	Description
	<p>Processing for the task that was last executed finished, but the migration of some files or directories failed. Use the Download Report dialog box or the <code>arcresultctl</code> command to check the message that was output when the migration failed, resolve the problem, and then execute the task again. Note that, when you execute the task again, files and directories that are not subject to the applicable policy will not be migrated.</p> <p>Failed to start(Message ID) An attempt to execute the task failed.</p> <p>Interrupted Task processing was interrupted because of one of the following reasons: a maximum duration, or interruption; or the file system was unmounted. If the task is interrupted repeatedly, change the maximum duration value.</p>
Progress	<p>The progress of the migration task when Last Migration Status is <code>Executing</code>. Migration tasks are processed in the following order:</p> <p>Waiting The task is waiting until another migration task is completed.</p> <p>Initializing Migration has started.</p> <p>Pre-processing (nn/mm) The progress of the pre-processing is displayed.</p> <p>Processing filters (nn/mm) The progress of the filter processing is displayed.</p> <p>Transferring data (nn/mm) The progress of the data transfer is displayed.</p> <p>Post-processing (nn/mm) The progress of the post-processing is displayed.</p> <p>Note that, if Last Migration Status is not <code>Executing</code>, <code>--</code> is displayed.</p>
Next Start Time	The date and time when the next migration task is to be executed next time.
Last End Time	<p>The date and time when the migration task that was last executed finished.</p> <p>If no migration task was executed, <code>--</code> is displayed.</p>
Number of Targets	<p>The total number of files and directories to be migrated by the migration task.</p> <p>Note that, if Progress is <code>Waiting</code>, <code>Initializing</code>, <code>Pre-processing</code>, or <code>Processing filters</code>, <code>0</code> is displayed.</p>
Number of Successful Migrations	The total number of files and directories that were successfully migrated.

Item	Description
Number of Failed Migrations	The total number of files and directories that could not be migrated.
Total Size of Files Migrated Successfully	The total size of files that were successfully migrated (in MB).
Total Size of Files That Failed to Be Migrated	The total size of files that were could not be migrated (in MB).
Work Space Used	<p>The amount of used work space when the migration task was run (in GB).</p> <p>Note that, if the migration task is running or the Active File Migration function is not being used, <code>--</code> is displayed. In addition, when the capacity of the work space is insufficient, <code>Overflowed</code> is displayed. When an error occurs in the work space, <code>Failed to obtain the amount of used space</code> is displayed.</p>
Task Comment	The comment.
Interval	The interval at which the migration task is executed.
Maximum Duration	The maximum duration for the migration task.
Task Status	<p>Indicates whether a migration task is enabled.</p> <p><code>Enabled</code></p> <p style="padding-left: 40px;">The migration task is enabled.</p> <p><code>Disabled</code></p> <p style="padding-left: 40px;">The migration task is disabled.</p>
Migration Results	Information about the migration task.
	<p>Successful</p> <p>Detailed information about the files and directories that were successfully migrated.</p> <p>New File</p> <p style="padding-left: 40px;">The number of files that were created.</p> <p>Data Changes</p> <p style="padding-left: 40px;">The number of files whose data was changed.</p> <p>Attribute Changes</p> <p style="padding-left: 40px;">The number of files for which only the attribute was changed.</p> <p>Directories</p> <p style="padding-left: 40px;">The number of directories.</p>
	<p>Failed</p> <p>If you click the <code>Details information</code> link, information about the failed migration task is displayed.</p> <p>For details about the Failed dialog box that appears when you click the <code>Details information</code> link, see Failed dialog box on page C-12.</p>

Policy Details subtab

You can use the **Policy Details** subtab to view the detailed information about the migration policy.

Table C-4 Items displayed on the Policy Details subtab of the Task Information tab in the migration-task page

Item	Description
Policy ID	The policy ID.
Filter condition	<p>If you click the Condition link, a list of selection conditions for the files set for the policy is displayed.</p> <p>For details about the Policy Information dialog box that appears when you click the Condition link, see Policy Information dialog box on page C-13.</p>

History tab

You can use the **History** tab to view the migration history.

Table C-5 Items displayed on the History tab in the migration-task page

Item	Description
History Data	<p>From the history data, select, from the drop-down list box, the data to be displayed in the graph.</p> <p>All Select to display all data.</p> <p>File Count Select to display the number of files that were migrated.</p> <p>File Size Select to display the size of the files that were migrated.</p>
Time Range	<p>Select, from the drop-down list box, the period for which history data is to be displayed in the graph.</p> <p>Past 1 week Select to display data for the past one week.</p> <p>Past 1 month Select to display data for the past one month.</p> <p>Past 3 months Select to display data for the past three months.</p> <p>Past 6 months Select to display data for the past six months.</p> <p>Past 1 year Select to display data for the past one year (365 days).</p>
Download all data as csv file	Click this to download a CSV file containing history data of the past one year (365 days).

Download Report dialog box

You can use the **Download Report** dialog box to download a list of the files and directories whose migration succeeded or failed (text file in UTF-8 format).

To open the **Download Report** dialog box, click **Download Report** on the **Task Details** subtab of the *migration-task* page in the **Migration Tasks** dialog box.



Note:

- If you stop a task that is currently executing, only the files and directories that have been migrated at the time that the task is stopped will be recorded.
- Files whose paths contain multi-byte characters other than Unicode (UTF-8) characters will not be correctly recorded.

Table C-6 Items displayed on the Download Report dialog box



Item	Description
Migration results list	Select the radio button corresponding to the report to be downloaded. List of successful migrations Select to download a list of files and directories that were successfully migrated. List of failed migrations Select to download a list of files and directories whose migration failed.
Download button	Download the report that was selected for Migration results list .



Failed dialog box

You can use the **Failed** dialog box to check a failed migration task.

To open the **Failed** dialog box, on the *migration-task* page in the **Migration Tasks** dialog box, click the *Details* information link of **Failed** on the **Task Details** subtab of the **Task Information** tab.

Table C-7 Items displayed on the Failed dialog box

Item	Description
Rows/Page	Select, from the drop-down list box, the maximum number of rows to be displayed on a page.
Page	When information is displayed on multiple pages, specify, in the text box, the page number of the page you want to view. Alternatively, click  or  to move to the previous or

Item	Description
	following page, respectively. Similarly, click  or  to move to the first or last page, respectively.
Message ID	The message ID of the message that includes the cause of the failure when the migration of files and directories fails.
Count	The total number of files and directories whose migration failed due to the cause included in the message indicated by Message ID .

Policy Information dialog box

You can use the **Policy Information** dialog box to view, add, or edit the selection conditions for files that are set for the policy. A maximum of 20 selection conditions can be set for a policy.

The following shows how to open the **Policy Information** dialog box:


- On the *migration-task* page in the **Migration Tasks** dialog box, click the **Condition** link of **Filter condition** on the **Policy Details** subtab of the **Task Information** tab.
- Click **Add** or **Edit** on the **4. Policy Settings** page of the Migration Task Wizard.
- Click **Condition** on the **5. Confirmation** page of the Migration Task Wizard.

Table C-8 Items displayed on the Policy Information dialog box

Item	Description
Attribute	Displays the type of selection condition for files.
Conditions	Displays the comparison operator used for a selection condition for files.
Value	Displays the value of a selection condition for files.
Add button	You can add a selection condition by specifying the selection condition by using the drop-down list boxes and text boxes under this button, and then clicking Add . Each selection condition consists of the following items in the given order: Attribute , Condition , and Value . For details about the values that can be specified for each item, see Table C-9 Selection conditions that can be specified on page C-14 .
Edit button	You can edit a selection condition by selecting the condition to be edited from the list, using the drop-down list boxes and text boxes under this button to specify the selection condition, and then clicking Edit . Each selection condition consists of the following items in the given order: Attribute , Condition , and Value . For details about the values that can be specified for each

Item	Description
	item, see Table C-9 Selection conditions that can be specified on page C-14 .
Delete button	You can delete the selected selection condition.

Table C-9 Selection conditions that can be specified

Attribute	Conditions	Value
File Extension	is is not	Specify the file extensions by using no more than 4,095 bytes. Do not include a period (.). Upper-case and lower-case letters are distinguished.
File Name	is is not	Specify a file to be moved or not moved using no more than 4,095 bytes. Upper-case and lower-case letters are distinguished. Only Unicode (UTF-8) characters are searched for as multibyte characters.
Directory Path	starts with does not start with	Specify an absolute path of the directory, using no more than 4,073 bytes. Upper-case and lower-case letters are distinguished. All files under the specified directory are targeted for migration. For example, specify <code>example/tmp</code> when targeting files under <code>/mnt/fs01/example/tmp/</code> . Only Unicode (UTF-8) characters are searched for as multibyte characters.
Last Accessed Time (atime)# Last Change Time (attributes change time (ctime)), Last Modified Time (data modification time (mtime))	is (in local time of the node) is not (in local time of the node) before (in local time of the node) after (in local time of the node)	One of the following options is selected to determine. Specify a specific date and time. Select a date using the  icon to the right. Specify relative date and time based on the current date and time. See the followed example and the files that are targeted in the case of the migration start date and time is at 12:30:00 on March 6. <code>is Now-5 day(s)</code> : The files of 12:30:00 on March 1 <code>after Now-3 hour(s)</code> : The files of 9:30:01 on March 6 or later <code>before Now-0 day(s)</code> : The files of 12:29:59 on March 6 or earlier

Attribute	Conditions	Value
File Size	is is not greater than less than	Specify the file size by using an integer consisting, and then select a unit (BYTE , KB , MB , or GB) from the drop-down list box. For the file size, specify an integer in one of the following ranges depending on the unit: - BYTE : 1 to 1,125,899,906,842,624 - KB : 1 to 1,099,511,627,776 - MB : 1 to 1,073,741,824 - GB : 1 to 1,048,576
Type of Change	is is not	Select a data modification type (Created , Data was changed , or Attribute was changed) from the drop-down list box.
#: WORM files cannot be searched by access time because retention periods are set for the <code>atime</code> of WORM files. For details about WORM files, see the <i>File System Protocols (CIFS/NFS) Administrator's Guide</i> .		

Migration Task Wizard

You can use the Migration Task Wizard to create or edit a migration task. A maximum of 10 tasks can be set for a file system.

To open the Migration Task Wizard, click **Add Task** in the **Migration Tasks** dialog box. Alternatively, select the name of the task to be edited, and then click **Edit Task**. When the Migration Task Wizard appears, the **1. Introduction** page is displayed first.

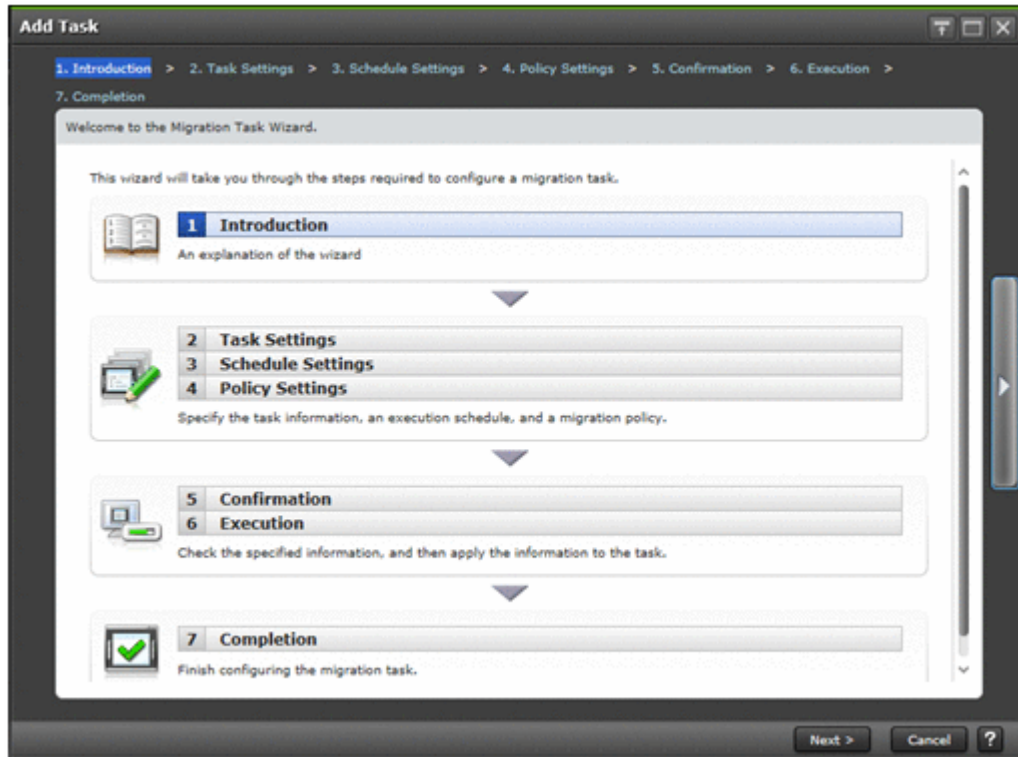


Table C-10 Pages shown for the Migration Task Wizard

Page	Description	See
1. Introduction	Check the information shown, and then click Next > .	N/A
2. Task Settings	Specify the necessary information, and then click Next > .	2. Task Settings page on page C-17
3. Schedule Settings	Specify the necessary information, and then click Next > .	3. Schedule Settings page on page C-17
4. Policy Settings	Specify the necessary information, and then click Next > .	4. Policy Settings page on page C-18
5. Confirmation	Check the displayed information, select the Yes, I have confirmed the above settings. check box, and then click Apply .	N/A
6. Execution	After settings have been configured, the 7. Completion page is automatically displayed.	N/A
7. Completion	Check the displayed information, and then click Finish .	N/A

Note: N/A = Not applicable.

2. Task Settings page

You can use this page to specify the name of the migration task and other information.


Table C-11 Items displayed on the 2. Task Settings page in the Migration Task Wizard

Item	Description
File system name	Specify the name of the file system. You can also select a file system from the File Systems dialog box (File Systems dialog box on page C-19) that appears when you click Select File System . Note that you cannot change this setting if you are editing an existing migration task.
Task name	Specify the name of the migration task by using no more than 32 characters. You can use alphanumeric characters and underscores (_). Specify a name that is unique in the file system. Note that you cannot change this setting if you are editing an existing migration task.
Task comment	Specify a comment by using no more than 256 bytes. You can use any alphanumeric character, exclamation mark (!), hash mark (#), dollar sign (\$), percent sign (%), ampersand (&), single quotation mark ('), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), colon (:), semicolon (;), left angle bracket (<), equal sign (=), right angle bracket (>), question mark (?), at mark (@), left square bracket ([), right square bracket (]), caret (^), underscore (_), grave accent mark (`), left curly bracket ({), vertical bar (), right curly bracket (}), tilde (~), space, and multi-byte characters that are encoded in UTF-8.
Priority	Select, from the drop-down list box, the priority level of the migration task to be executed according to a schedule. High Select to specify High. The number 3 will be set as the numerical priority level. Middle Select to specify Middle. The number 5 will be set as the numerical priority level. Low Select to specify Low. The number 7 will be set as the numerical priority level.

3. Schedule Settings page

You can use this page to specify the schedule of the migration task.

Table C-12 Items displayed on the 3. Schedule Settings page in the Migration Task Wizard

Item	Description
Start date	Select the date on which the migration task will be run for the first time, by using the icon  on the right.
Start time	To run on a specific date and time, specify the time in <i>HH:MM</i> format. Be sure to specify a time in the future.
Interval	Specify the interval at which the migration task is to be run, by specifying a value in the range from 10 minutes to 1 month. Note that, if the target file system is a home-directory-roaming file system (for which the default setting is 1 hour) or read-write-content-sharing file system (for which the default setting is 10 minutes), you cannot change the default value to a value exceeding 1 hour.
Maximum Duration	Specify the time at which the migration task will be interrupted, by specifying a value in the range from 0 to 60 hours. If you do not want to specify a time, specify 0. Note that, if the target file system is a home-directory-roaming file system or read-write-content-sharing file system, you cannot change the value from the default setting (0).

4. Policy Settings page

You can use this page to specify migration policies. The maximum number of migration policies is 10. If you do not specify a policy, all files will be migrated. Note that, if the target file system is a home-directory-roaming file system or read-write-content-sharing file system, you cannot set any migration policies.

Table C-13 Items displayed on the 4. Policy Settings page in the Migration Task Wizard

Item	Description	See
Policies	The policy ID of the specified policy. If no policy is specified, <i>No Data</i> is displayed.	N/A
Add button	Adds a policy.	Policy Information dialog box on page C-13
Edit button	Edits the settings of the selected policy.	Policy Information dialog box on page C-13
Delete button	Deletes the selected policy.	N/A





Note: N/A = Not applicable.

File Systems dialog box

You can use the **File Systems** dialog box to select a file system.

To open the **File Systems** dialog box, click **Select File System** on the **2. Task Settings** page of the Migration Task Wizard.

Table C-14 Items displayed on the File Systems dialog box

Item	Description
Column Settings button	Sets the columns to be displayed. In the dialog box that appears when you click Column Settings , select the columns you want to display, and then click OK . Note that, if you click Restore Default Settings , all columns will be selected.
Rows/Page	Select, from the drop-down list box, the maximum number of rows to be displayed on a page.
Page	When information is displayed on multiple pages, specify, in the text box, the page number of the page you want to view. Alternatively, click  or  to move to the previous or following page, respectively. Similarly, click  or  to move to the first or last page, respectively.
Name	The name of the file system.
Mount Status	The status of the file system. Online (RW) The file system is mounted with both read and write operations permitted. Online (RO) The file system is mounted as read-only. Unmounted The file system is unmounted. Expanding The file system is being expanded or an error occurred during expansion processing. Wait a while, and then refresh the processing node information. If the status does not change, an error might have occurred during processing. Obtain all the log data, and then inform maintenance personnel. Reclaiming The unused area of the virtual LUs that are used for the file system is being released. Data corrupted The file system is blocked because of an error in the OS or a pool capacity shortage. Take corrective action by referring to the <i>Single Node Troubleshooting Guide</i> . Device error The file system is blocked because of an error in the LU (multiple drive failure).

Item	Description
	Take corrective action by referring to the <i>Single Node Troubleshooting Guide</i> . Unknown error Information about the file system could not be obtained.
Namespace Type	Displays how the file system is linked to the HCP system. File System The file system is linked to the HCP system at the file system level. Subtree The file system is linked to the HCP system at the share level.
Target Namespace	The namespace for the HCP system to which data will be migrated.

Stop Task dialog box

You can use the **Stop Task** dialog box to stop a migration task.

To open the **Stop Task** dialog box, click **Stop Task** on the **Migration Tasks** dialog box.

Table C-15 Items displayed on the Stop Task dialog box

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-3 Items displayed on the Task Details subtab of the Task Information tab in the migration-task page on page C-8
Apply	After selecting the I have read the above warning , you can stop the migration task.	N/A
Note: N/A = Not applicable.		

Migrate Immediately dialog box

You can use the **Migrate Immediately** dialog box to immediately run a migration task.

To open the **Migrate Immediately** dialog box, click **Migrate Immediately** on the **Migration Tasks** dialog box.

Table C-16 Items displayed on the Migrate Immediately dialog box

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-3 Items displayed on the Task Details subtab of the Task Information tab in the migration-task page on page C-8
Apply	After selecting the I have confirmed the above settings. you can immediately run a migration task.	N/A
Note: N/A = Not applicable.		

Enable Task dialog box

You can use the **Enable Task** dialog box to enable a migration task.

To open the **Enable Task** dialog box, click **Enable Task** in the **Migration Tasks** dialog box or on the *migration-task* page in the **Migration Tasks** dialog box.

Table C-17 Items displayed on the Enable Task dialog box

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-3 Items displayed on the Task Details subtab of the Task Information tab in the migration-task page on page C-8
Information about the migration task.	After selecting the I have read the above warning. you can enable a migration task.	N/A
Note: N/A = Not applicable.		

Disable Task dialog box

You can use the **Disable Task** dialog box to disable a migration task.

To open the **Disable Task** dialog box, click **Disable Task** in the **Migration Tasks** dialog box or on the *migration-task* page in the **Migration Tasks** dialog box.

Table C-18 Items displayed on the Disable Task dialog box

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-3 Items displayed on the Task Details subtab of the Task Information tab in the migration-task page on page C-8
Apply	After selecting the I have confirmed the above settings. you can disable a migration task.	N/A
Note: N/A = Not applicable.		

Delete Task dialog box

You can use the **Delete Task** dialog box to delete a migration task.

Note that, if the target file system is a home-directory-roaming file system or read-write-content-sharing file system, you cannot delete the migration task or its policies.

To open the **Delete Task** dialog box, click **Delete Task** on the **Migration Tasks** dialog box.

Table C-19 Items displayed on the Delete Task dialog box

Item	Description	See
Migration Task Information	Information about the migration task.	Table C-3 Items displayed on the Task Details subtab of the Task Information tab in the migration-task page on page C-8
Apply	After selecting the I have read the above warning. you can delete a migration task.	N/A
Note: N/A = Not applicable.		

System Configuration Wizard

The **System Configuration Wizard** allows you to configure a system.

To display the **System Configuration Wizard**, click the **Action** menu in the top-left corner of the GUI, and then choose **Configuration Wizards–System Configuration Wizard**.

Table C-20 Pages displayed in the System Configuration Wizard

Pages	Description
1. Introduction	Check the contents displayed on the page, and then click Next .
2. License Settings	Set the license for using the HDI software, and then click Next . There are two ways to set the license key: specifying a license key file, and directly entering a license key string into the dialog box. Note that this page does not appear if the System Configuration Wizard is displayed by using the Provisioning Wizard .
3. Basic Settings	Specify the following information, and then click Next . <ul style="list-style-type: none"> Registering node network information: host name^{#1}, system management IP address, netmask or prefix length, IP address of the default gateway (optional) When Use DHCP is selected, you can use DHCP to assign the system management IP address, netmask, and IP address of the default gateway.^{#2} Registering the DNS server^{#2}: IP address of the primary server (optional when Use DHCP is selected), IP address of the secondary server (optional), default domain name (optional) Setting the time on the node: Specify a time zone and then either specify the NTP server name, or specify the time manually. Encryption setting: When an encryption license is set, select whether to encrypt the local data (internal hard disks) or the data to be stored in the HCP system.^{#3#4}
4. Confirmation	Check the information displayed on the page, select the check box, and then click Apply .
5. Execution	Displays the execution status of system configuration.
6. Completion	Make sure that the processing results are correct, and then click Finish .
<p>#1: Specify a host name that has 15 or fewer characters. You can use alphanumeric characters and hyphens (-). The host name must begin with an alphabetic character, and must not end with a hyphen (-). System-reserved words cannot be specified regardless of the case of letters. For system-reserved words, see List of reserved words on page E-2. In the initial settings, a unique name is assigned to each node.</p> <p>#2: If you are using DHCP and the DNS server is already registered to the DHCP server, the information obtained from the DHCP server is set as the DNS server information. In this case, manually specified information is ignored.</p> <p>#3: If the common key used for local data encryption is corrupted or cannot be obtained, user data will no longer be available. We recommend that you use the <code>encdisplaykey</code> command to display the key, and save the key on external media.</p>	

Pages	Description
	#4: If the common key used for HCP payload encryption is corrupted or cannot be obtained, you will not be able to migrate data to the HCP system or to recall data from the HCP system. Be sure to use the <code>hcpdisplaykey</code> command to display the key, and then save the key on external media.

Service Configuration Wizard

The **Service Configuration Wizard** allows you to configure a service.

To display the **Service Configuration Wizard**, click the **Action** menu in the top-left corner of the GUI, and then choose **Configuration Wizards–Service Configuration Wizard**.

Table C-21 Pages displayed in the Service Configuration Wizard

Pages	Description
1. Introduction	Check the content displayed on the page, and then click Next .
2. HCP Settings	<p>Select the check box when linking with the HCP system. Specify the HCP information, and then click Next.</p> <p>Registering HCP information: system name, tenant name, the host name or IP address that has been made external and is used to connect to the HCP system (if any relay device such as a load balancer is used when connecting the linked HCP system to the network), user name and password of the tenant administrator.</p> <p>To change the current tenant admin password, select Yes in the Change password, and then enter a new password. If the password is changed from HDI, the change is also applied in HCP. Make this change only if you want to change the settings in HCP. For details about changing passwords and the characters that can be used in a password, see the explanation in the Change HCP Tenant Admin Password dialog box (Change HCP Tenant Admin Password dialog box on page C-36).</p> <p>Specify the information for the replica HCP when using the replication functionality with the HCP system.</p> <p>After specifying the information, click the Test Connection to check the connection for communicating with the HCP system.</p> <p>Specify the following information when using a proxy server for communication between a node and HCP.</p> <p>Registering proxy server information: host name, port number, user name and password.</p>
3. Resource Settings	<p>Specify the file system information, and then click Next.</p> <p>Select whether to allocate file system capacity automatically or manually. If you want to link with HCP through a share, manually allocate the file system capacity.</p> <p>Next, in the Create File Systems area, click Add and specify information required for each file system. For details about information that can be specified, see Table C-163 Items displayed in the Create File System dialog box on page C-215.</p>

Pages	Description
<p>4. CIFS User Authentication Settings</p>	<p>Specify the CIFS user authentication information, and then click Next.</p> <p>Select Active Directory authentication, local authentication by the node OS, or another authentication method as the method for CIFS user authentication.</p> <p>An authentication method that is neither Active Directory authentication nor local authentication by the node OS can be selected if a domain controller within the domain authenticates users when IPv4 is used. In this case, after the wizard is finished, set the appropriate information in the Access Protocol Configuration dialog box.</p> <p>The information specified when Active Directory authentication or local authentication is selected is as follows:</p> <p>When Active Directory authentication is selected</p> <p>Specify the DNS name as well as the user name and password for the domain controller. To modify settings such as the NetBIOS name for the domain or the user mapping method, select Custom Settings, and then enter the following information:</p> <ul style="list-style-type: none"> • DNS name • NetBIOS name for the domain[#] • Server name or IP address of the domain controller (You can specify as many as 5, separated by commas.)[#] • Name and password of the domain controller user • User mapping method (RID, Active Directory schema, or other)[#] <ul style="list-style-type: none"> - For RID: Specify the system-wide range for user IDs and group IDs. Then, in the Domain Range area, click Setting, and then specify up to 256 domains and their ID ranges. Register no more than 20 domains each time. If more than 20 domains are registered at the same time, a timeout might occur. Register all domains that have been specified as Active Directory domains. If you only register domains that have trust relationships, the users on those domains are not allowed access to the CIFS share. - For Active Directory schemas: Select Microsoft services for Unix or RFC 2307 schema as the method for obtaining user IDs or group IDs from the domain controller. - For other methods: When using LDAP user mapping, after the wizard has finished set up the mapping in the Access Protocol Configuration dialog box. <p>When local authentication is selected</p> <ul style="list-style-type: none"> • Workgroup name • User name and user ID (optional) • Name and ID of the group to which the user belongs (optional) • User password (optional)
<p>5. Confirmation</p>	<p>Check the content displayed on the page, select the check box, and then click Apply.</p>

Pages	Description
6. Execution	Displays the execution status of a service configuration.
7. Completion	Make sure that the processing results are correct, and then click Finish .
<p>#: Specify this item when Custom settings is selected or when you want to change the current settings. If Custom settings is not selected, the NetBIOS name of the domain and up to five DC servers are automatically searched for and set, based on the DNS name of the specified domain. When only the CIFS protocol is used, RID user mapping is selected and an ID range from 70,000 through 4,069,999 (4 million IDs) is set for the NetBIOS name of the domain that is automatically detected. When both the CIFS and NFS protocols are used, the user mapping that uses Active Directory schema is selected, and the RFC2307 schema is used for acquiring user IDs and group IDs from the domain controller.</p>	

Download Chargeback Report dialog box

You can use the **Download Chargeback Report** dialog box to download statistics from an HCP system, including the number of times it has been accessed by an HDI system or tenant capacity usage.



Note: Information for each tenant is obtained from the HDI system. For details about chargeback reports, contact the administrator of the HCP system.

To display the **Download Chargeback Report** dialog box, click the **Action** menu in the top-left corner of the GUI, and then choose **Chargeback Report**.

Table C-22 Items displayed in the Download Chargeback Report dialog box

Item	Description
Report interval	Specifies the interval at which statistics are acquired. Daily Obtains the daily status. Hourly Obtains the hourly status.
Start date	Specifies the start date of the period for which information is downloaded.
End date	Specifies the end date of the period for which information is downloaded.
Download button	Downloads information. A dialog for specifying the download destination is displayed.

Import Files dialog box

You can import files from the shared directory on the another file server to the shared directory in the HDI system.

To display the **Import Files** dialog box, in the top-left corner of the GUI, choose **Action**, and then **Import Files**.



Tip: A maximum of 20 tasks for importing files can be executed at the same time.

Table C-23 Operations that can be performed in the Import Files dialog box

Operation	Description	See
Defining tasks	You can define tasks for importing data. Specify information, such as a shared directory in the HDI system to which files are to be imported, or the file server where the files to be imported are stored.	Table C-24 Items specified when a task is defined on page C-27
Verifying files	You can verify whether the source files can be imported.	Table C-25 Items displayed when files are verified on page C-29
Starting the importation of files	You can import files on another file server to the HDI system.	Table C-26 Items displayed when importation of files starts on page C-31
Checking files for which an error occurred	You can check whether there were any errors or cautions while files were being verified or imported.	Table C-27 Items displayed in the Scan Failure List dialog box, the Import Failure List dialog box, or the Read Failure List dialog box on page C-33 Table C-29 Items displayed in the Warning List dialog box on page C-34

Table C-24 Items specified when a task is defined

Item	Description
Import target	Host name Specify an HDI node to which files are to be imported.
	Share name Specify a shared directory in the HDI system to which files are to be imported. Use the Select Share button to select the shared directory.
	Export point The path to the shared directory is displayed.
Import source	Host name Specify the host where the files to be imported are stored.
	Protocol Select the protocol used for importing data.

Item	Description
	<p>Share name Specify the shared directory where the files to be imported are stored.</p> <p>User name If CIFS is selected for Protocol, specify a user name to be used for connecting to the CIFS share where the files to be imported are stored. Specify the user name using no more than 256 characters. You can use alphanumeric characters.</p> <p>Password If CIFS is selected for Protocol, specify a password to be used for connecting to the CIFS share where the files to be imported are stored. Specify the password using no more than 128 characters. You can use alphanumeric characters.</p> <p>Test Connection button Checks whether the file share that has been specified as the import-source is accessible.</p>
CIFS Share Settings	<p>Name resolution If CIFS is selected for Protocol, specify how to access the files to be imported. The system automatically switches the authentication method. Local authentication, Active Directory authentication, and the default account are used to access files in that order.</p> <p>Mapping file Select this check box when you want to specify a mapping file. Check the local accounts on the file server in which the files to be imported are stored. Then create a mapping file beforehand that is to be used for using those accounts in the HDI system. For details about how to create a mapping file, see Importing data from another file server by using the CIFS protocol on page 3-7.</p> <p>Default account If CIFS is selected for Protocol, specify the default account. When the file owner accounts or the accounts set in ACEs for the files have been deleted from the file server environment in which the files to be imported are stored, this default account is assigned instead of the deleted accounts. Do not use Does not set any account to be assigned instead of the deleted accounts. User Assigns a user account instead of the deleted accounts. Group Assigns a group account instead of the deleted accounts.</p> <p>Account If User or Group is selected for Default account, specify the account name to be assigned in the HDI system. If you use a domain account, specify it in the format <i>domain-name\account-name</i>.</p>

Item	Description
Show Plan button	<p>Allows you to check the specified settings. It also specifies the task name.</p> <p>If the displayed settings and the task name are correct, click the Start Scan button to verify whether the files can be imported.</p> <p>If the settings for the task are changed after the files are verified, you can click the Start Import button to start the importing of the files.</p> <p>When you click the Start Scan button or the Start Import button, the Warning List dialog box might be displayed (Table C-29 Items displayed in the Warning List dialog box on page C-34). Follow the displayed instructions.</p>
Task name	<p>Specify the task name using no more than 1,024 bytes. Alphanumeric characters, symbols, and Unicode (UTF-8) multi-byte characters can be used. Click the Show Plan button, and then specify this in the displayed window.</p>

Table C-25 Items displayed when files are verified

Item	Description	
Task name	Displays the task name.	
Status	<p>Displays the current status of the task.</p> <p>Scanning Whether the files can be imported is being verified.</p> <p>Scan finished Verification of the files finished.</p> <p>Scan stopped Verification of the files was stopped.</p>	
Progress	Displays the progress of the task.	
	Details	<p>Displays the detailed current status of the task.</p> <p>Total Displays the total number of files to be verified.</p> <p>Scanned Displays the number of files for which verification was executed and the percentage (%) of those files among all the files to be verified.</p> <p>Pending Displays the number of files for which verification has not been executed yet and the percentage (%) of those files among all the files to be verified.</p> <p>Scan Success</p>

Item	Description
	<p>Displays the number of files successfully verified and the percentage (%) of those files among all the files to be verified.</p> <p>Read Failure</p> <p>Displays the number of files that could not be recognized as verification targets.</p> <p>Scan Failure</p> <p>Displays the number of files for which verification failed and the percentage (%) of those files among all the files to be verified.</p> <p>Start time</p> <p>Displays the date and time verification started.</p> <p>Elapsed time</p> <p>Displays the time elapsed since the verification started.</p> <p>Completion time</p> <p>Displays the date and time verification finished.</p>
Display Scan Failure List button	<p>Displays a list of files for which errors occurred during verification. Clicking this button displays the Scan Failure List dialog box (Table C-27 Items displayed in the Scan Failure List dialog box, the Import Failure List dialog box, or the Read Failure List dialog box on page C-33).</p>
Display Read Failure List button	<p>Displays a list of files that could not be recognized as verification targets. Clicking this button displays the Read Failure List dialog box (Table C-27 Items displayed in the Scan Failure List dialog box, the Import Failure List dialog box, or the Read Failure List dialog box on page C-33).</p>
More Actions	<p>Click ▼ and choose the necessary operation.</p> <p>Download Scan Failure List</p> <p>Downloads a text file that contains a list of files for which errors occurred during verification.</p> <p>Download Read Failure List</p> <p>Downloads a text file that contains a list of files that could not be recognized as verification targets.</p>
Settings	<p>Displays information (that was specified when the task was defined) of the shared directory to which the files are to be imported and of the file server in which the files to be imported are stored.</p>
CIFS Share Settings	<p>Displays the settings that were specified when the task was defined and that are used for importing data in the CIFS share.</p>
Start Import button	<p>Starts importing files. This button becomes active after the verification of the files to be imported finishes.</p>
Edit Settings & Start Import button	<p>Changes the task settings. Clicking this button displays the items shown in Table C-24 Items specified when a task is defined on page C-27. Check and, if necessary, revise the settings. Then, click the Show Plan button and make sure that the settings are correct. Next,</p>

Item	Description
or Edit Settings & Retry Scan button	click the Start Import button to start importing files or click the Start Scan button to re-execute verification of the files to be imported. When you click the Start Scan button or the Start Import button, the Warning List dialog box might be displayed (Table C-29 Items displayed in the Warning List dialog box on page C-34). Follow the displayed instructions. You can click this button when Status is <code>Scan finished</code> or <code>Scan stopped</code> . If you want to change the task settings, wait until verification finishes, or click the Cancel Scan button to cancel verification.
Cancel Scan button	Cancels the verification of the files to be imported.

Table C-26 Items displayed when importation of files starts

Item	Description
Task name	Displays the task name.
Status	Displays the current status of the task. <code>Importing</code> Files are being imported. <code>Importing(Temporary On-Demand)</code> The import method has been temporarily changed to on-demand importing because migration to the HCP system was started or the file system free capacity on the import target reached the threshold. <code>Import finished</code> Importing files finished. <code>Import stopped</code> Importing files from another file server was stopped. <code>Maintenance required</code> An error occurred. Check the details about the error, and take actions for recovery. <code>On-demand</code> Only the files accessed by clients are imported on demand.
Progress	Displays the progress of the task. Details Displays the detailed current status of the task. Total Displays the total number of files to be imported. Imported Displays the number of files for which import processing has been executed and the percentage (%) of those files among all the files to be imported. Pending Displays the number of files for which import processing has not been executed yet and the

Item	Description
	<p>percentage (%) of those files among all the files to be imported.</p> <p>Import Success Displays the number of files successfully imported and the percentage (%) of those files among all the files to be imported.</p> <p>Read Failure Displays the number of files that could not be recognized as import sources.</p> <p>Import Failure Displays the number of files for which importing failed and the percentage (%) of those files among all the files to be imported.</p> <p>Start time Displays the date and time the importation started.</p> <p>Elapsed time Displays the time elapsed since the import started.</p> <p>Completion time Displays the date and time the import finished.</p>
<p>Display Import Failure List button</p>	<p>Displays a list of files for which errors occurred during the import. Clicking this button displays the Import Failure List dialog box (Table C-27 Items displayed in the Scan Failure List dialog box, the Import Failure List dialog box, or the Read Failure List dialog box on page C-33).</p>
<p>Display Read Failure List button</p>	<p>Displays a list of files that could not be recognized as import sources. Clicking this button displays the Read Failure List dialog box (Table C-27 Items displayed in the Scan Failure List dialog box, the Import Failure List dialog box, or the Read Failure List dialog box on page C-33).</p>
<p>More Actions</p>	<p>Click ▼ and choose the necessary operation.</p> <p>Download Import Failure List Downloads a text file that contains a list of files for which errors occurred during the import.</p> <p>Download Read Failure List Downloads a text file that contains a list of files that could not be recognized as import sources.</p>
<p>Settings</p>	<p>Displays information (that was specified when the task was defined) of the shared directory to which the files are to be imported and of the file server in which the files to be imported are stored.</p>
<p>CIFS Share Settings</p>	<p>Displays the settings that were specified when the task was defined and that are used for importing data in the CIFS share.</p>

Item	Description
Edit Settings & Retry Import button	<p>Changes the task settings. Clicking this button displays the items shown in Table C-24 Items specified when a task is defined on page C-27. Check and, if necessary, revise the settings. Then, click the Show Plan button and make sure that the settings are correct. Next, click the Start Import button to re-execute importation of the source files. When you click the Start Import button, the Warning List dialog box might be displayed (Table C-29 Items displayed in the Warning List dialog box on page C-34). Follow the displayed instructions.</p> <p>You can click this button when Status is <code>On-demand</code> or <code>Import stopped</code>. If you want to change the task settings, click the Change to On-Demand Import button to change the import method or click the Cancel Import button to cancel the importing of the files.</p>
Cancel Import button	<p>Cancels the importing of files from another file server.</p>
Change to On-Demand Import button	<p>Changes the import method to on-demand importing. If you click this button to change the import method, only the source files that are requested by a client are imported when the client accesses the files.</p> <p>You can click this button when Status is <code>Importing</code> or <code>Importing(Temporary On-Demand)</code>.</p>

Table C-27 Items displayed in the Scan Failure List dialog box, the Import Failure List dialog box, or the Read Failure List dialog box

Item	Description	
Summary area	Fatal Error	Displays the number of files for which fatal errors occurred.
	Error	Displays the number of files with a severity level of error or higher (error or fatal error level).
	Warning	Displays the number of files with a severity level of warning or higher (warning, error, or fatal error level).
	Information	Displays the number of files with a severity level of information or higher (any of all levels).
Failure List area	Severity	<p>Displays the severity level for the error. Clicking this item displays the Failure Detail dialog box (Table C-28 Items displayed in the Failure Detail dialog box on page C-34).</p> <ul style="list-style-type: none"> • <code>Fatal Error</code>: Fatal error level • <code>Warning</code>: warning level • <code>Error</code>: Error level • <code>Information</code>: Information level
	Time	Displays the time the error or warning occurred.
	File	Displays the path to the file for which the error or warning occurred.
	Description	Displays an overview of the error or warning.

Item	Description
Download button	Downloads the text file that contains a list of files for which an error or warning occurred.

Table C-28 Items displayed in the Failure Detail dialog box

Item	Description
Host name	Displays the HDI node to which the files are to be imported.
Share name	Displays the shared directory of the HDI system to which the files are to be imported.
File	Displays the path to the file for which an error or warning occurred.
Severity	Displays the severity level of the error.
Time	Displays the time the error or warning occurred.
Message ID	Displays the corresponding message ID.
Description	Displays an overview of the error or warning.
Recovery Action	Displays the action to be taken for the error.

Table C-29 Items displayed in the Warning List dialog box

Item	Description
Message ID	Displays the message ID indicating the contents of the warning.
Description	Displays an explanation.
Edit Settings button	Changes the task settings. Clicking this button displays the items shown in Table C-24 Items specified when a task is defined on page C-27 .
Start Scan button	Verifies whether the files can be imported. This button is displayed if the Warning List dialog box is displayed while you are verifying files.
Start Import button	Starts the importing of the files. This button is displayed if the Warning List dialog box is displayed while you are importing files.

Configure Proxy Server dialog box

This dialog box allows you to specify information about the proxy server to be used for communication between nodes and HCP.

To display the **Configure Proxy Server** dialog box, click the **Action** menu in the top-left corner of the GUI, and then choose **Configure Proxy Server**.

Table C-30 Items displayed in the Configure Proxy Server dialog box

Item		Description
Proxy server	Use	Select this if you want to use a proxy server for communication between nodes and HCP.
	Host name	Specify the host name of the proxy server.
	Port	Specify the port number to be used on the proxy server.
	User authentication	User name
Password		If you are using a proxy server that requires user authentication, specify the password. The entered password is displayed by using asterisks (*).

Change System Admin Password dialog box

In the **Change System Admin Password** dialog box, a system administrator can change his or her own password.



Note: The password set here is required for the operation and management of the HDI system. Be sure not to forget this password.

The password is shared with the HDI API administrator account. If the password is changed from the GUI, use the new password in the API. If the current password is lost, use the `adminpasswd` command to initialize the password and then specify a new password.

To display the **Change System Admin Password** dialog box, click the **Action** menu in the top-left corner of the GUI, choose **Change Password**, and then choose **Change System Admin Password**.

Table C-31 Items displayed in the Change System Admin Password dialog box

Item	Description
User name	Displays the user name.
Current password	Enter the current password. The entered password is displayed by using asterisks (*).
New password	Enter a new password by using 256 or fewer characters. If you specify two or more words as a password, delimit the words by a space. You can use alphanumeric characters and the following symbols: ! # \$ % & ' () * + - . = @ \ ^ _ Specify a new password that meets conditions set in the Login Security dialog box, such as the minimum number of characters and combination of the characters that can be used as a password. For

Item	Description
	details about the Login Security dialog box, see Login Security dialog box on page C-38 . The entered password is displayed by using asterisks (*).
Confirm new password	Enter the character string you entered for New password . The entered password is displayed by using asterisks (*).

Change HCP Tenant Admin Password dialog box

The HCP tenant admin password can be changed.

If the password is changed from HDI, the change is also applied in HCP. Make this change only if you want to change the settings in HCP.



Note:

- The specified password is necessary to connect to HCP tenants. Do not forget this password.
- Change the tenant administrator password when no migration or recall is taking place. If a migration or recall takes place when a password change is in progress, the migration or recall processing might fail.
- If you specify a password that includes invalid characters, after the processing to change the password fails, the original password might become unusable. In such a case, ask the HCP administrator to issue a new password. After receiving a new password from the HCP administrator, reconfigure the tenant administrator user account by using the **Service Configuration Wizard** ([Service Configuration Wizard on page C-24](#)).
- If a tenant or tenant administrator user account is shared with another HDI system, it is necessary to update the appropriate setting on the HDI system, so that the changed password is also used on the system. If such a password change is made, report the new password to the administrator of the other HDI system, and then ask the administrator to update the relevant HCP information registered in the HDI system.
- If a tenant or tenant administrator user account is shared with another HDI system, make a password change after verifying that no migration or recall is taking place on the other HDI system.

If an HDI system exists where a migration or recall cannot be stopped, ask the HCP administrator to create and configure a new user account for the tenant administrator. After changing the password of the new user account, report the new user name and password to the administrator of the HDI system by using the same user account. When the tenant administrator user account is configured for each relevant HDI, ask the HCP administrator to delete the old user account.

To display the **Change HCP Tenant Admin Password** dialog box, click the **Action** menu in the top-left corner of the GUI, choose **Change Password**, and then choose **Change HCP Tenant Admin Password**.

Table C-32 Items displayed in the Change HCP Tenant Admin Password dialog box

Item	Description
User name	Displays the current user name.
Current password	Enter the current password. The entered password is displayed by using asterisks (*).
New password	Enter a new password by using 64 or fewer characters. Only alphabetic characters, numeric characters, and symbols can be used in passwords. Of these three types of characters, use at least two to specify the password. In addition, multibyte Unicode (UTF-8) characters can also be used. The password can contain space characters, but cannot consist of space characters only. The specified password of a tenant administrator user account must meet all of the password requirements, including the minimum number of characters and the combination of characters. For information about the password requirements for a tenant administrator user account, check with the HCP administrator. The entered password is displayed by using asterisks (*).
Confirm new password	Enter the character string you entered for New password . The entered password is displayed by using asterisks (*).
Yes, I have read the above description and want to change the HCP tenant admin password. check box	Select this check box if you want to Change the Password.

Update HCP Anywhere Credentials dialog box

This dialog box allows you to change the password to be used for accessing HCP Anywhere.

To display the **Update HCP Anywhere Credentials** dialog box, click the **Action** menu in the top-left corner of the GUI, choose **Change Password**, and then choose **Update HCP Anywhere Credentials**.

Table C-33 Items displayed in the Update HCP Anywhere Credentials dialog box

Item	Description
Password	Enter a new password. The entered password is displayed by using asterisks (*).

Login Security dialog box

You can change the timeout time, automatic account lock-related settings, and password policy for a system administrator account.

To display the **Login Security** dialog box, in the top-left corner of the GUI, choose **Action** and then **Login Security**.

Table C-34 Items displayed in the Login Security dialog box

Item		Description
Session timeout		Specify the session timeout time in minutes. If you do not want to limit the timeout time, specify 0.
Password policy	Enable account lockout	<p>Select Yes check box to enable auto-locking of accounts.</p> <p>An account will be locked when the number of consecutive unsuccessful log on attempts exceeds the number specified in Maximum number of login attempts.</p> <p>Maximum number of login attempts</p> <p>Specify the number of consecutive unsuccessful log on attempts allowed before an account is locked. The specified value must be in the range from 1 to 100.</p> <p>Time at which to cancel account lockout</p> <p>Specify the length of time (in minutes) before unlocking the automatically locked account. The specified value must be in the range from 1 to 999.</p>
	Minimum length	Specify the minimum number of characters for a password in the range from 1 to 256.
	Minimum number of characters	<p>Specify the conditions for the combinations of characters that can be used for a password.</p> <p>Uppercase</p> <p>Specify the minimum number of uppercase characters that must be included in a password in the range from 0 to 256. If you do not want to limit the number of uppercase characters, specify 0.</p> <p>Lowercase</p> <p>Specify the minimum number of lowercase characters that must be included in a password in the range from 0 to 256. If you do not want to limit the number of lowercase characters, specify 0.</p> <p>Numbers</p> <p>Specify the minimum number of numeric characters that must be included in a password in the range from 0 to 256. If you do not want to limit the number of numeric characters, specify 0.</p>

Item		Description
		Symbols Specify the minimum number of symbols that must be included in a password in the range from 0 to 256. If you do not want to limit the number of symbols, specify 0.
	Minimum number of words	Specify the minimum number of words that can be specified as a password in the range from 1 to 128.

Check for Errors dialog box

A system administrator can check the error information for the nodes in the **Check for Errors** dialog box.

To display the **Check for Errors** dialog box, click the **Action** menu in the top-left corner of the GUI, and then choose **Launch-Check for Errors**.

List of RAS Information page

You can select the error information to be checked.

The **List of RAS Information** page first appears after the **Check for Errors** dialog box is displayed.

From the **Info. type** drop-down list, select the error information you want to display.

Table C-35 Error information selected from the Info. type drop-down list on the List of RAS Information page

Item	Description
List of messages	Displays the list of error messages. Important messages about errors that occurred in the hardware and software are output to the system message log.
List of system logs	Displays the list of system logs.
List of other log files	Displays log files other than system messages and system logs.
Batch-download	Displays log groups for batch downloading or batch deleting log files.
List of core files	Displays a list of core and dump files.
Server check	Displays the connection status between a node and an external server.

List of RAS Information page (for List of messages)

The **List of RAS Information** page (for `List of messages`) displays the system message. For the system message, important messages related to errors occurring in the hardware or software are output.

To view past system messages, select a file for list generation from the **Files** drop-down list, and then click the **Display** button on the right of the page. To narrow down the displayed messages by severity level, select the severity level from the **Conditions** drop-down list, and then click the **Display** button on the right of the page.

To display the **List of RAS Information** page (for `List of messages`), in the **Check for Errors** dialog box, select **List of messages** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Table C-36 Items displayed on the List of RAS Information page (for List of messages)

Item	Description
Info. type drop-down list	Select the type of information to be displayed. For details about the items displayed, see Table C-35 Error information selected from the Info. type drop-down list on the List of RAS Information page on page C-39 .
Files drop-down list	Select the message file to be displayed. <ul style="list-style-type: none">• em_alertfile Displays the latest error messages.• em_alertfile.generation-number Displays messages about past errors. Saved messages, such as em_alertfile.1 or em_alertfile.2, can be selected. The larger the generation number, the older the messages. Note that 0 might be suffixed to the file name, depending on the system status.
Conditions drop-down list	Narrow down the messages to be displayed by severity level. <ul style="list-style-type: none">• Information Select this option to display messages at the information and higher levels (all levels).• Warning Select this option to display messages at the warning and higher levels (warning, error, and fatal error levels).• Error Select this option to display messages at the error and higher level (error and fatal error levels).• Fatal error Select this option to display messages at the fatal error level only.
Display button	Displays the messages.
Importance	Displays messages by severity level. <ul style="list-style-type: none">• Information

Item	Description
	<p>The information message.</p> <ul style="list-style-type: none"> • Warning The warning message. • Error The error message. • Fatal error The fatal error message.
Date and time	Displays the date and time when the message was output.
Message text	Displays the message text.
Message ID	Displays the message ID.
Download button	Download the system messages of the displayed generation.
Delete button	Delete the system messages of the displayed generation.

List of RAS Information page (for List of system logs)

The **List of RAS Information** page (for `List of system logs`) displays the system log.

To view past system log files, select a past file from the **Displayed files** drop-down list, and then click **Display**.

To display the **List of RAS Information** page (for `List of system logs`), in the **Check for Errors** dialog box, select **List of system logs** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Table C-37 Items displayed on the List of RAS Information page (for List of system logs)

Item	Description
Displayed files drop-down list	<p>Select the system log file you want to display.</p> <p>syslog Displays the latest system log file.</p> <p>syslog.generation-number Displays a past system log file.</p> <p>A saved system log file, such as syslog.1 or syslog.2, can be selected. The larger the generation number, the older the system log file. Note that 0 might be suffixed to the file name, depending on the system status.</p>
Display button	Displays the system logs.
Contents	The contents of the system log file are displayed.
Download button	Download the currently displayed system log files.

Item	Description
Delete button	Delete the currently displayed system log files.

List of RAS Information page (for List of other log files)

The **List of RAS Information** page (for `List of other log files`) displays the log files that are not system messages or system logs.

When you select the type of log file from the **File type** drop-down list and then click **Display**, the latest information for the selected log file is displayed. To view past log files, select a specific past file from the **Displayed files** drop-down list, and then click **Display**. For past log files, a generation number is added to the end of the name or before the file extension. The larger the generation number becomes, the older the log file.

To display the **List of RAS Information** page (for `List of other log files`), in the **Check for Errors** dialog box, select **List of other log files** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Table C-38 Items displayed on the List of RAS Information page (for List of other log files)

Item	Description
File type drop-down list	Select the type of the log file you want to display.
Displayed files drop-down list	Select the log file you want to display.
Display button	Displays the log files.
Contents	The contents of the log file selected from the File type drop-down list and the Displayed files drop-down list are displayed.
Download button	Download the log files of the displayed generation.
Delete button	Delete the log files of the displayed generation. Note that Delete is not displayed for some log files, and you cannot delete these log files.

List of RAS Information page (for Batch-download)

You can download and delete log files in a batch operation.

To display the **List of RAS Information** page (for `Batch-download`), in the **Check for Errors** dialog box, select **Batch-download** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Table C-39 Items displayed on the List of RAS Information page (for Batch-download)

Item	Description
Radio button	Select a log group to download.
Log group	Displays log names of groups.
File type	Displays the types of log files that belong to a log group.
Number of files	Displays the total number of log files currently saved (the total number of the latest log file and the past log files).
Explanation	Displays the description of a log file.
Download button	Batch download all past log files that belong to the log group selected. In batch downloading, log files are archived by <code>tar</code> and compressed by <code>gzip</code> . When you perform batch downloading, some data might be missed if the disk selected to store the Temporary Internet files folder for Internet Explorer has insufficient space. In this situation, Internet Explorer does not generate an error or message.
Delete button	Batch delete all past log files that belong to the log group selected.

List of RAS Information page (for List of core files)

The **List of RAS Information** page (for `List of core files`) displays core files and dump files.

To display the **List of RAS Information** page (for `List of core files`), in the **Check for Errors** dialog box, select **List of core files** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.



Note:

- Expired core files are deleted automatically. If a core file is generated, download it and send it to maintenance personnel.
- Delete downloaded core files manually.
- The dump files are listed along with the core files if the OS dump files are output. A dump file is required only when the vendor requests you to collect dump files. In such a case, download dump files and then contact maintenance personnel. Also, there are three levels of dump files, 1, 3, and 4. The names of dump files contain a string such as the following:
`lvdump-file-level (1, 3, or 4)`
Maintenance personnel can obtain level 1 files, but cannot obtain level 3 or 4 files because they contain access data for the file system (NFS and CIFS services). Depending on the error level, you might be asked by maintenance personnel to collect dump files, but since level 3 and 4 dump files contain user information, be especially careful when managing these files.

- If the displayed dump files are not the latest files, a dialog box displaying the following message appears: "The displayed dump files are not the latest files." If this happens, download the latest dump files as follows:
 1. Download all of the displayed dump files.
 2. Confirm that the download finished successfully, and then delete all of the dump files. When you delete the downloaded dump files, output of the latest dump files starts. The output of dump files will take some time.
 3. Confirm that the latest dump files are output, and then download all of the dump files.

Note that, if you run the `nnreset` command after deleting the downloaded dump files but before the output of the latest dump files finishes, the new dump files will not be collected by the `nnreset` command.

Confirm that the latest dump files are output, and be sure to run the `nnreset` command only after all of the dump files have been downloaded.

Table C-40 Items displayed on the List of RAS Information page (for List of core files)

Item	Description
Core file name	Displays the name of a core file.
Size (KB)	Displays the core file size.
Created at	Displays the date and time the core file was created.
Available space for core files	Displays the available space in MB for storing core files on the OS disk and the usage ratio as a percentage. If space is insufficient, old unnecessary core files and downloaded core files are deleted.
Download button	Download the core file and dump file selected.
Delete button	Delete the core file and dump file selected.
Transfer All Files button	Transfers all core files and dump files to the FTP server in a batch operation. Clicking this button displays the Transfer All Files page (Transfer All Files page on page C-45).
Delete All Files button	Delete all core files and dump files.

List of RAS Information page (for Server check)

You can check the status of the connections with the external servers.

To display the **List of RAS Information** page (for `Server check`), in the **Check for Errors** dialog box, select **Server check** from the **Info. type** drop-down list on the **List of RAS Information** page, and then click **Display**.

Table C-41 Items displayed on the List of RAS Information page (for Server check)

Item	Description
Results	Can be used to check the status of the connections between the nodes and the external servers. For details about the content, see the description about the <code>log_interfaces_check</code> file in the <i>Single Node Troubleshooting Guide</i> .

Transfer All Files page

You can transfer to the FTP server all log files on a node in a batch operation.

Specify the necessary information, and then click **Transfer** to download all core files and dump files in batch.

To display the **Transfer All Files** page, click **Transfer All Files** on the **List of RAS Information** page (for `List of core files`).

Note:

In some cases, such as when many files to be transferred exist, processing might take a long time, and an error might occur in Internet Explorer. If such cases occur, disable the SmartScreen filter function in Internet Explorer temporarily, and then execute the processing again.

Table C-42 Items displayed on the Transfer All Files page

Item	Description
FTP Server	Specify the IP address or the host name of the FTP server.
User name	Specify the name of the user who logs on to the FTP server.
Password	Specify the password of the user.
Directory	Specify the directory of the transfer destination. You cannot specify a character string including non-ASCII characters. Create a directory on the FTP server before transferring files.
Transfer button	Transfer all log files to the FTP server in a batch operation.

Dashboard tab

In the **Dashboard** tab, a system administrator can understand the overall status of the system.

To display the **Dashboard** tab, choose **Dashboard** in the top-left corner of the GUI.

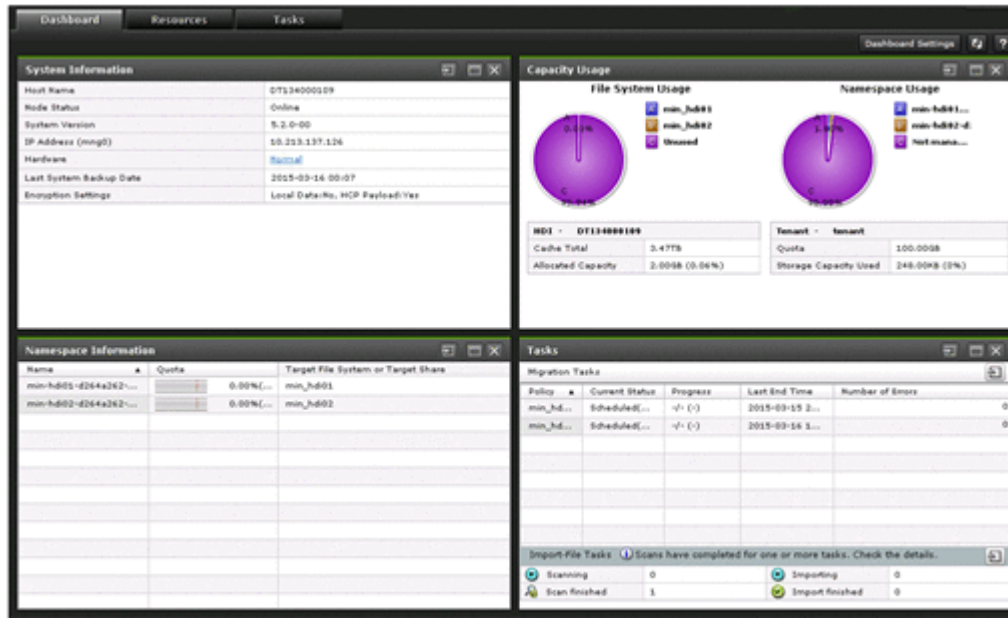


Table C-43 Items displayed in the Dashboard tab

Item	Description	See
Dashboard Settings button	Click this button to change the panels displayed in the Dashboard tab.	Panel Configuration dialog box on page C-50
System Information	Displays information such as the node status and system version.	System Information panel on page C-46
Capacity Usage	Displays the file system and namespace capacities.	Capacity Usage panel on page C-47
Namespace Information	Displays the information about the namespace used by the managed HDI system.	Namespace Information panel on page C-48
Tasks	Displays the progress of the migration and importing of files.	Tasks panel on page C-49

System Information panel

The **System Information** panel displays the node status.

Table C-44 Items displayed in the System Information panel






Item	Description
	Clicking this icon displays the <i>host-name</i> window (host-name window on page C-51).
or	Click to maximize the panel. Click to return the panel to the size before it was maximized.

Item	Description
Host Name	Displays the host name of the node.
Node Status	<p>Displays the node status.</p> <p>Online The node is running normally.</p> <p>Online Pending The node is starting up.</p> <p>Offline The node is stopped.</p> <p>Offline Pending The node is shutting down.</p> <p>Partial Online Some services have been stopped.</p> <p>Error An error occurred. Take action according to the error information.</p>
System Version	Displays the system version.
IP Address (mng0)	Displays the IP address of the node.
Hardware	<p>Displays the hardware status.</p> <p>Normal The hardware is running normally.</p> <p>Error An error occurred. Take action according to the error information.</p> <p>Unknown error An error occurred for which information cannot be obtained.</p>
Last System Backup Date	<p>Displays the date and time the system configuration information was saved.</p> <p>Displays <code>Now saving</code> if the system configuration information is being saved. Displays <code>Not saving</code> if the system configuration information is not saved.</p>
Encryption Settings	<p>Displays whether encryption is enabled for the local data and the data to be stored in the HCP system, when an encryption license is set.</p> <p>Local Data: <code>Yes</code> or <code>No</code>, HCP Payload: <code>Yes</code> or <code>No</code></p>

Capacity Usage panel

The **Capacity Usage** panel displays the file system and namespace capacities.






Table C-45 Items displayed in the Capacity Usage panel

Item		Description
		Clicking this icon displays the File Systems window (File Systems window on page C-56).
 or 		Click  to maximize the panel. Click  to return the panel to the size before it was maximized.
File System Usage	Pie graph	Displays the capacity allocated to file systems as usage.
	Table	<p>HDI -host-name Displays the host name for HDI.</p> <p>Cache Total Displays the total capacity of volume groups that can be used for file systems. The specified file system size includes the size of the work space used by the Active File Migration function and the Large File Transfer function. As a result, the size of the file system that can actually be used is smaller than the specified size.</p> <p>Allocated Capacity Displays the amount of total volume group capacity allocated to file systems and work spaces as a percentage.</p>
Namespace Usage	Pie graph	Displays namespace usage.
	Table	<p>Tenant - tenant-name Displays the tenant name.</p> <p>Quota Displays the total capacity of the tenant.</p> <p>Storage Capacity Used Displays the tenant capacity usage.</p>

Namespace Information panel

The **Namespace Information** panel displays the information about the namespace used by the managed HDI system.

Table C-46 Items displayed in the Namespace Information panel







Item	Description
	Clicking this icon displays the <i>tenant-name</i> window (tenant-name window on page C-79).
 or 	Click  to maximize the panel. Click  to return the panel to the size before it was maximized.
Name	Displays the name of the namespace used by the managed HDI file system or file share.


Item	Description
Quota	Displays the namespace capacity values in a bar graph. The percentage of capacity used is displayed within the bar graph. If a namespace is used only for viewing (read only) the data of other HDI systems, two hyphens (--) are displayed.
Target File System or Target Share	Displays the name of the file system or file share to which the namespace is allocated.

Tasks panel

The **Tasks** panel displays the progress of the migration and importing of files.

Table C-47 Items displayed in the Tasks panel

Item	Description	
	Clicking this icon displays the Import Files window (Import Files window on page C-81).	
 or 	Click  to maximize the panel. Click  to return the panel to the size before it was maximized.	
Migration Tasks		Clicking this icon displays the Migration Tasks dialog box (Migration Tasks dialog box on page C-4).
	Task	Displays the name of the migration task.
	Current Status	Displays the current status of the migration. <p>Executing</p> <p>The task is executing.</p> <p>Finished normally</p> <p>The task that was last executed ended successfully.</p> <p>Partially failed</p> <p>Processing for the task that was last executed finished, but the migration of some files or directories failed. Use the Download Report dialog box or the <code>arcresultctl</code> command to check the message that was output when the migration failed, resolve the problem, and then execute the task again. Note that, when you execute the task again, files and directories that are not subject to the applicable policy will not be migrated.</p> <p>Failed to start(Message ID)</p> <p>An attempt to execute the task failed.</p> <p>Interrupted</p> <p>Task processing was interrupted because of one of the following reasons: a maximum duration,</p>

Item		Description
		or interruption; or the file system was unmounted. If the task is interrupted repeatedly, change the maximum duration value.
	Progress	<p>The progress of the migration task. Migration tasks are processed in the following order:</p> <p>Waiting The task is waiting until another migration task is completed.</p> <p>Initializing Migration has started.</p> <p>Pre-processing (nn/mm) The progress of the pre-processing is displayed.</p> <p>Processing filters (nn/mm) The progress of the filter processing is displayed.</p> <p>Transferring data (nn/mm) The progress of the data transfer is displayed.</p> <p>Post-processing (nn/mm) The progress of the post-processing is displayed.</p>
	Last End Time	Displays the date and time the last executed migration task finished.
	Number of Failed Migrations	Displays the total number of files and directories for which migration failed for the most recent migration task displayed.
Import-File Tasks		Clicking this icon displays the Import Files window (Import Files window on page C-81).
	Task status	<p>Displays the number of tasks in each of the following statuses among the tasks for importing files from another file server:</p> <p>Scanning Whether the files can be imported is being verified.</p> <p>Scan finished Verification of the files finished.</p> <p>Importing Files are being imported.</p> <p>Import finished Importing of files has finished.</p>

Panel Configuration dialog box

To use **Panel Configuration** dialog box, you can change the panels displayed in the **Dashboard** tab.

To display the **Panel Configuration** dialog box, click the **Dashboard Settings** button in the **Dashboard** tab.

Table C-48 Items displayed in the Panel Configuration dialog box

Item	Description
System Information	Displays the System Information panel in the Dashboard tab.
Capacity Usage	Displays the Capacity Usage panel in the Dashboard tab.
Namespace Information	Displays the Namespace Information panel in the Dashboard tab.
Tasks	Displays the Tasks panel in the Dashboard tab.

host-name window

The *host-name* window displays the operating status of an HDI system.

To display the *host-name* window, select **Resources** in the top-left corner of the GUI, and then click a host name in the tree on the left side of the GUI.

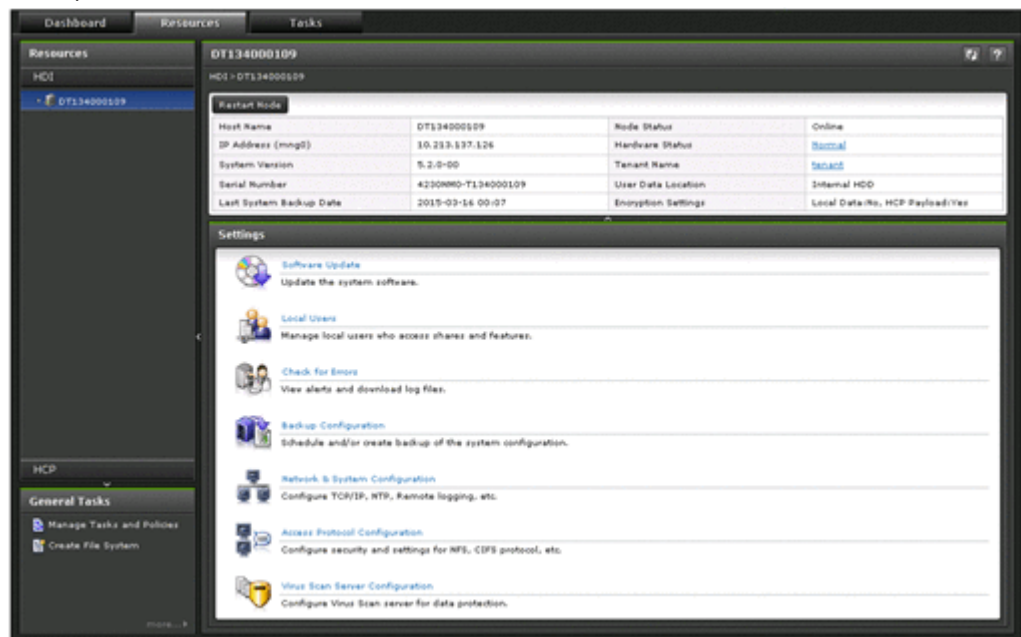


Table C-49 Items displayed in the host-name window

Item	Description
Restart Node button	Restarts the node, and displays the Restart Node dialog box (Restart Node dialog box on page C-84).
Host Name	Displays the host name.
IP Address (mng0)	Displays the IP address.

Item	Description
System Version	Displays version information for the system.
Serial Number	Displays the device identification number.
Last System Backup Date	<p>Displays the date and time when the system configuration information is saved.</p> <p>Displays <code>Now saving</code> if the system configuration information is being saved. Displays <code>Not saving</code> if the system configuration information is not saved.</p>
Node Status	<p>Displays the node status.</p> <p><code>Online</code></p> <p>The node is running normally.</p> <p><code>Online Pending</code></p> <p>The node is starting up.</p> <p><code>Offline</code></p> <p>The node is stopped.</p> <p><code>Offline Pending</code></p> <p>The node is shutting down.</p> <p><code>Partial Online</code></p> <p>Some services have been stopped.</p> <p><code>Error</code></p> <p>An error occurred. Take action according to the error information.</p>
Hardware Status	<p>Displays the hardware status.</p> <p><code>Normal</code></p> <p>The hardware is running normally.</p> <p><code>Error</code></p> <p>An error occurred. Take action according to the error information.</p> <p><code>Unknown error</code></p> <p>An error occurred for which information cannot be obtained.</p>
Tenant Name	Displays the tenant name.
User Data Location	<p>Displays the storage location of the user data.</p> <p><code>Internal HDD</code></p> <p>Stored on the internal hard disk.</p> <p><code>Storage system</code></p> <p>Stored in storage systems.</p> <p><code>Internal HDD and Storage system</code></p> <p>Stored on the internal hard disk and in storage systems.</p>
Encryption Settings	<p>Displays whether encryption is enabled for the local data and the data to be stored in the HCP system, when an encryption license is set.</p> <p><code>Local Data:Yes or No, HCP Payload:Yes or No</code></p>

	Item	Description
Settings area	Software Update	Updates the software running on the node. Clicking this menu displays the System Software Installation dialog box (System Software Installation dialog box on page C-85).
	Local Users	Manages the information about the users who can access a file system. Clicking this menu displays the Local Users dialog box (Local Users dialog box on page C-85).
	Check for Errors	Checks the error information for the node. Clicking this menu displays the Check for Errors dialog box (Check for Errors dialog box on page C-39).
	Backup Configuration	Downloads the system configuration file and uploads the downloaded system configuration file. Clicking this menu displays the Backup Configuration dialog box (Backup Configuration dialog box on page C-97).
	Network & System Configuration	Changes the network and system configurations. Clicking this menu displays the Network & System Configuration dialog box (Network & System Configuration dialog box on page C-103).
	Access Protocol Configuration	Performs operations such as changing the client authentication method. Clicking this menu displays the Access Protocol Configuration dialog box (Access Protocol Configuration dialog box on page C-137).
	Virus Scan Server Configuration	Registers the scan server and sets scan conditions for real-time scans. Clicking this menu displays the Virus Scan Server Configuration dialog box (Virus Scan Server Configuration dialog box on page C-186).

Shares window

The **Shares** window displays a list of file shares.

To display the **Shares** window, select **Resources** in the top-left corner of the GUI, select the triangle icon next to a host name in the tree on the left side of the GUI, and then click **Shares**.

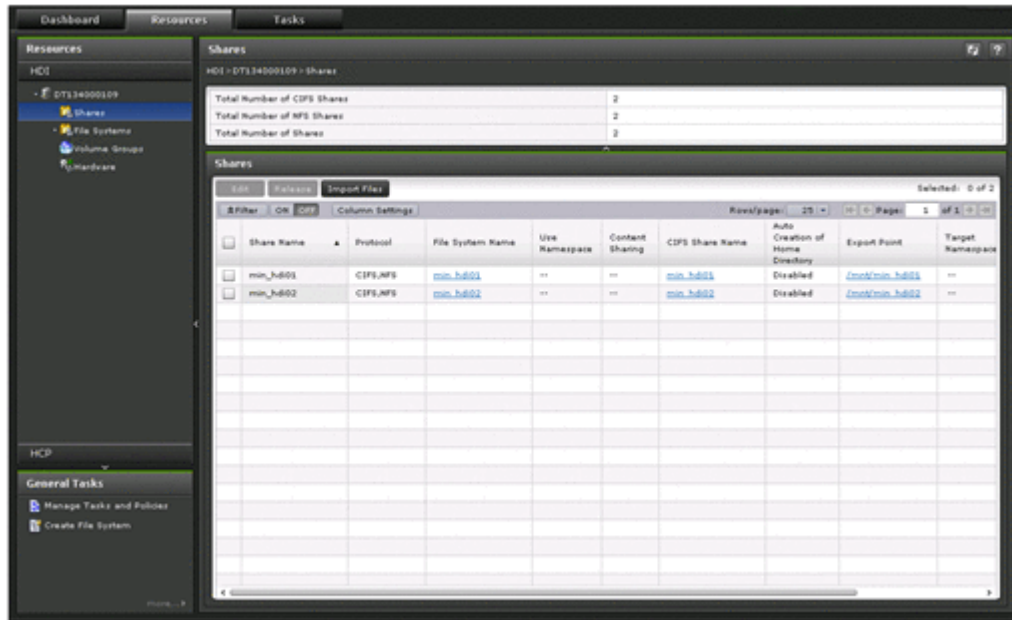


Table C-50 Items displayed in the Shares window

Item		Description
Total Number of CIFS Shares		Displays the total number of CIFS shares.
Total Number of NFS Shares		Displays the total number of NFS shares.
Total Number of Shares		Displays the total number of file shares.
Shares area	Edit button	Click this button to change the file share settings. Clicking this button displays the Edit Share dialog box (Edit Share dialog box on page C-198).
	Release button	Click this button to release a file share. Clicking this button displays the Release Share(s) dialog box (Release Share(s) dialog box on page C-204).
	Import Files button	Click this button to import files from another file server. Clicking this button displays the Import Files dialog box (Import Files dialog box on page C-27). You cannot import files from other file servers to file shares created in file systems that share data with other HDI systems via a linked HCP system.
	Share Name	Displays share names.
	Protocol	Displays the protocol used for a file share. CIFS The CIFS protocol is used. NFS The NFS protocol is used. CIFS, NFS Both the CIFS and NFS protocols are used.

Item	Description
File System Name	Displays the name of the file system in which the file share is created. Clicking the name of a file system opens the <i>file-system-name</i> window for the file system (file-system-name window on page C-61).
Use Namespace	Displays whether the HCP namespace is allocated to the share. If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.
Content Sharing	Displays how data is shared with other HDI systems via the linked HCP. Off Data is not being synchronized with other HDI systems. On (Read-Only) Data in other HDI systems is being referenced as read-only. If the share is not linked to the HCP system at the share level, two hyphens (--) are displayed.
File Share Capacity	The value of the capacity of the migration-destination namespace is displayed in a bar graph. The ratio of the currently used capacity (%) is displayed inside the bar graph. If the share capacity is not limited based on the hard quota of the migration-destination namespace, two hyphens (--) are displayed.
CIFS Share Name	Displays CIFS share names. Clicking a CIFS share name displays the CIFS Protocol Settings dialog box (CIFS Protocol Settings dialog box on page C-197). If the CIFS protocol is not used, two hyphens (--) are displayed.
Auto Creation of Home Directory	Displays whether the function for automatically creating a home directory is used in the CIFS share.
SMB Encryption	Displays whether the communication with the CIFS client is to be encrypted when you use SMB 3.0. Auto Communication with the client is to be encrypted only when the client supports encryption. Mandatory Communication with the client is always to be encrypted. Disabled Communication with the client is not to be encrypted. Inherit CIFS service default

Item	Description
	<p>The CIFS service configuration definitions are used.</p> <p>If the CIFS protocol is not used, two hyphens (--) are displayed.</p>
Export Point	<p>Displays the absolute path to the shared directory. Clicking the absolute path when the settings are specified to use the NFS protocol displays the NFS Protocol Settings dialog box (NFS Protocol Settings dialog box on page C-198).</p>
Target Namespace	<p>Displays the name of the namespace allocated to the share.</p> <p>To check the status of the migration-destination namespace, click <i>namespace-name</i> to display the <i>tenant-name</i> window (tenant-name window on page C-79).</p> <p>If the namespace is not allocated to the share, two hyphens (--) are displayed.</p>
External HCP Host Name	<p>If data in another HDI system is referenced as read-only at the share level, the host name or IP address that has been made external and is used to connect to the HCP system is displayed.</p> <p>If no host name or IP address is specified, two hyphens (--) are displayed.</p>
Namespace-access Account	<p>Displays the user name of the account used for viewing the migration-destination namespace.</p> <p>This item is displayed if data in other HDI systems is referenced as read-only or data is made available on other HDI systems via a linked HCP system at the share level.</p>
Replica System Name	<p>If replica HCP system information is specified at the share level, the name of the replica HCP system is displayed.</p>
External Replica HCP Host Name	<p>If replica HCP system information is specified at the share level, the host name or IP address that has been made external and is used to connect to the replica HCP system is displayed.</p> <p>If no host name or IP address is specified, two hyphens (--) are displayed.</p>

File Systems window

The **File Systems** window displays the status of all files systems.

To display the **File Systems** window, select **Resources** in the top-left corner of the GUI, select the triangle icon next to a host name in the tree on the left side of the GUI, and then click **File Systems**.

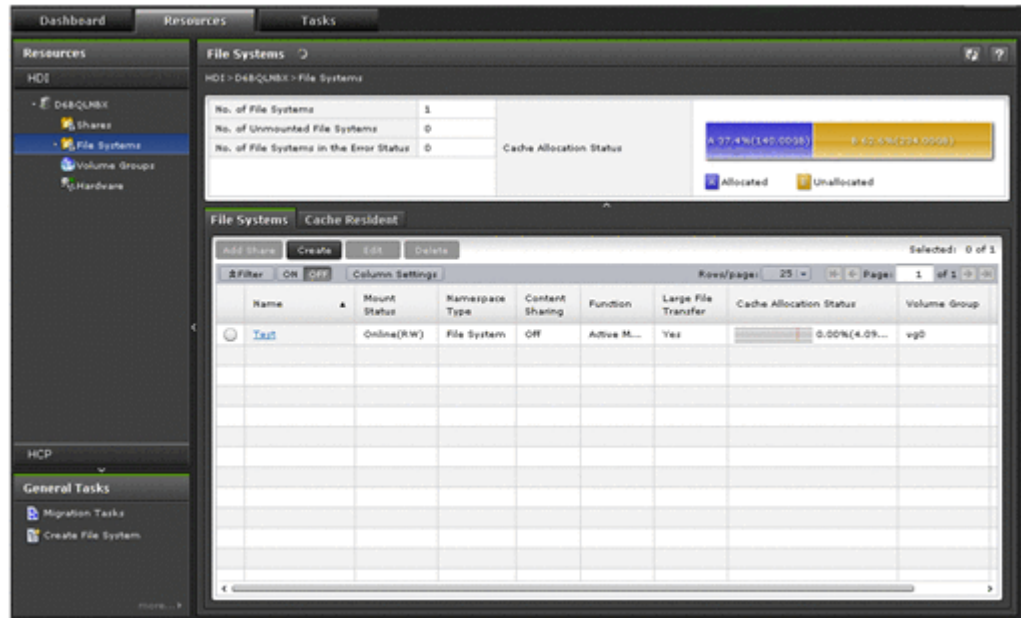


Table C-51 Items displayed in the File Systems window

Item	Description	See
No. of File Systems	Displays the total number of file systems.	--
No. of Unmounted File Systems	Displays the total number of unmounted file systems.	--
No. of File Systems in the Error Status	Displays the total number of file system for which errors have occurred.	--
Cache Allocation Status	Displays the amount of total volume group capacity allocated to file systems as a percentage.	--
File Systems tab	Displays an overview of settings and statuses for each file system, including the file system name and capacity.	File Systems tab on page C-57
Cache Resident tab	Cache resident information is displayed.	Cache Resident tab on page C-60

File Systems tab

The **File Systems** tab displays an overview of the settings and status of each file system.

Table C-52 Items displayed in the File Systems tab of the File Systems window

Item	Description
Add Share button	Adds a file share. Clicking this button displays the Add Share dialog box (Add Share dialog box on page C-208). Note that a file share cannot be added if a read-write-content-sharing file system or home-directory-roaming file system and a file share have already been created.
Create button	Creates a file system. Clicking this button displays the Create File System dialog box (Create File System dialog box on page C-215).
Edit button	Changes the settings for a file system. Clicking this button displays the Edit File System dialog box (Edit File System dialog box on page C-228).
Delete button	Deletes a file system. Clicking this button displays the Delete File System dialog box (Delete File System dialog box on page C-235).
Name	Displays the file system name. To check the status of a specific file system, click <i>file-system-name</i> to display the <i>file-system-name</i> window (file-system-name window on page C-61).
Mount Status	Displays the status of the file system. If an error has occurred, take necessary action according to the <i>Single Node Troubleshooting Guide</i> . Online (RW) The file system is mounted with read and write permissions. Online (RO) The file system is mounted as read-only. Data corrupted The file system is blocked. Unmounted The file system has been unmounted. Expanding Either the file system is being expanded, or an error occurred during processing. Wait a while and then update this information. If the status does not change, an error might have occurred during processing. Obtain all log files, and contact maintenance personnel. Device error The file system is blocked due to a drive failure. Unknown error An error occurred for which information cannot be obtained.
Namespace Type	Displays how the file system is linked to the HCP system.

Item	Description
	<p>File System The file system is linked to the HCP system at the file system level.</p> <p>Subtree The file system is linked to the HCP system at the share level.</p>
Content Sharing	<p>Displays how data is shared with other HDI systems via the linked HCP.</p> <p>Off Data is not being synchronized with other HDI systems.</p> <p>On (Read-Only) Data in other HDI systems is being referenced as read-only.</p> <p>On (Read/Write) Data is being shared among HDI systems by using the read-write-content-sharing functionality (read-write-content-sharing file system).</p> <p>Home directory Roaming among HDI systems is enabled for home directory data created for each end user (home-directory-roaming file system).</p>
Function	<p>Displays whether the WORM functionality has been enabled, and whether each functionality for HDI is used.</p> <p>None The WORM functionality has not been enabled, and no other functionality is used.</p> <p>WORM The WORM functionality is set.</p> <p>Active Migration The Active File Migration functionality is used.</p> <p>WORM, Active Migration The WORM functionality has been enabled, and the Active File Migration functionality is used.</p>
Large File Transfer	<p>Displays whether the Large File Transfer functionality is used.</p> <p>If the Content Sharing is other than <code>off</code>, two hyphens (<code>--</code>) are displayed.</p> <p>This item is displayed if the version of linked HCP system is 8.0 or later.</p>
Cache Allocation Status	<p>Displays the capacity currently used, and that allocated to file systems. If the file system is unmounted, <code>0.00% (0.00GB) Used</code> is displayed for the currently used capacity, and <code>0.00GB</code> is displayed for the capacity allocated to file systems.</p>

Item	Description
	The specified file system size includes the size of the work space used by the Active File Migration function and the Large File Transfer function. As a result, the size of the file system that can actually be used is smaller than the specified size.
Volume Group	Displays the name of a volume group used by the file system.
No. of Shares	Displays the number of file shares created in the file system.
Target Namespace	Displays the name of the HCP namespace set in the file system. To check the status of the migration-destination namespace, click <i>namespace-name</i> to display the <i>tenant-name</i> window (tenant-name window on page C-79).
External HCP Host Name	Displays the host name or IP address that has been made external and is used to connect to the HCP system. If no host name or IP address is set, two hyphens (--) are displayed.
External Replica HCP Host Name	Displays the host name or IP address that has been made external and is used to connect to the replica HCP system. If no host name or IP address is specified, two hyphens (--) are displayed.

Cache Resident tab

If cache resident policies are set up for pinning files in the cache, information related to cache residency is displayed in this tab. Information is displayed every time a task is executed according to a cache resident policy.

If information about pinned files is not set to be acquired, information related to cache residency will not be displayed. Only a message will be displayed.

Table C-53 Items displayed in the Cache Resident tab of the File Systems window

Item	Description
Name	Displays the file system name.
Pinned Capacity	Displays the total capacity of the pinned files.
% Pinned	Displays the percentage of the total file system capacity used by the pinned files.
Used Capacity	Displays the used capacity of the file system.
% Used	Displays the used capacity of the file system as a percentage (%).
Total Capacity	Displays the capacity allocated to the file system.

Item	Description
	The specified file system size includes the size of the work space used by the Active File Migration function and the Large File Transfer function. As a result, the size of the file system that can actually be used is smaller than the specified size.
As of	Displays the time at which the task executed for the cache resident policies is completed.

file-system-name window

The *file-system-name* window displays the status of a specific file system.

To display the *file-system-name* window, select **Resources** in the top-left corner of the GUI, select the triangle icon next to **File Systems** in the tree on the left side of the GUI, and then click a file system.

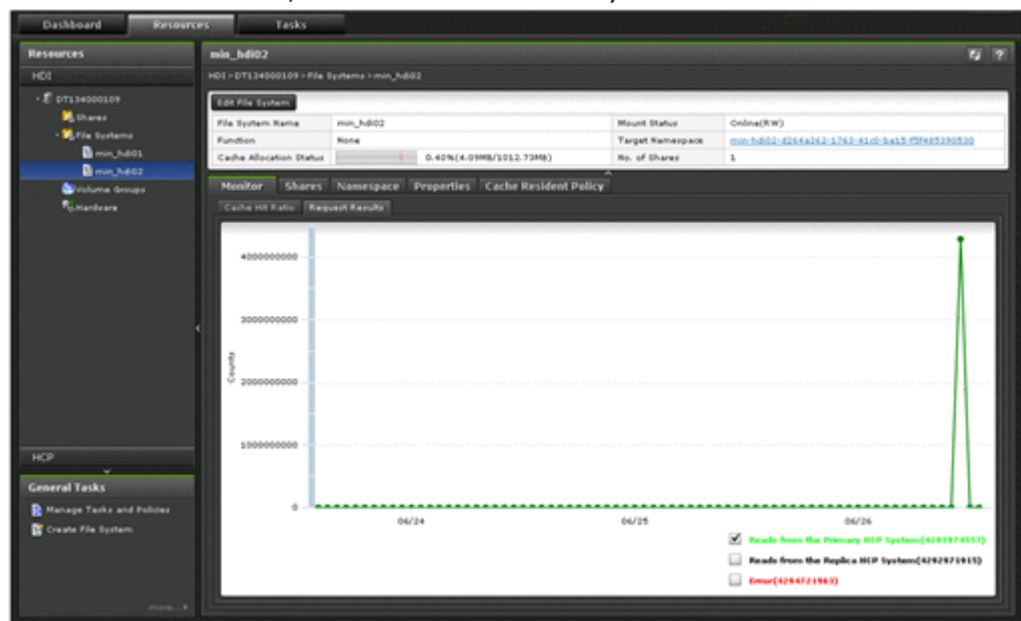


Table C-54 Items displayed in the file-system-name window

Item	Description	See
Edit File System button	Changes the file system settings. Clicking this button displays the Edit File System dialog box.	Edit File System dialog box on page C-228
File System Name	Displays the name of the file system.	--
Function	Displays whether WORM functionality has been set, and the name of the function that is using the file system. For details about the items displayed, see the description for Function in the File Systems tab (File Systems tab on page C-57).	--

Item	Description	See
Cache Allocation Status	Displays the capacity currently used, and that allocated to file systems. If the file system is unmounted, 0.00% (0.00GB) Used is displayed for the currently used capacity, and 0.00GB is displayed for the capacity allocated to file systems. The specified file system size includes the size of the work space used by the Active File Migration function and the Large File Transfer function. As a result, the size of the file system that can actually be used is smaller than the specified size.	--
Mount Status	Displays the status of the file system. For details about the items displayed, see the description for Mount Status in the File Systems tab (File Systems tab on page C-57).	--
Target Namespace	Displays the name of the HCP namespace set in the file system. To check the status of the migration-destination namespace, click <i>namespace-name</i> to display the <i>tenant-name</i> window (tenant-name window on page C-79).	--
No. of Shares	Displays the number of file shares created in the file system.	--
Monitor tab	Displays the usage of a client.	Monitor tab on page C-62
Shares tab	Displays file share settings.	Shares tab on page C-63
Namespace tab	Displays HCP namespace information.	Namespace tab on page C-65
Properties tab	Displays settings such as WORM and the file version restore functionality.	Properties tab on page C-67
Cache Resident Policy tab	Displays the settings for the cache resident policies.	Cache Resident Policy tab on page C-69

Monitor tab

The **Monitor** tab displays the usage of a client.

Table C-55 Items displayed in the Monitor tab of the file-system-name window

Item	Description
Cache Hit Ratio	Displays the percentage of times that a client accesses an HDI system file and is able to view that file without recalling data from an HCP system.

Item	Description
	<p>Note that data is recalled from the HCP system in 1 MB units. If the I/O for a file being temporarily accessed is less than 1 MB, then all subsequent access to the file might reference the file cached on the HDI system, instead of recalling the file again. This can cause the cache hit ratio to appear higher than it really is.</p> <p>When importing files from another file server, the cache hit ratio might appear lower than it really is until the file import process completes.</p>
Request Results	<p>Displays the number of times that data is recalled from an HCP system when a client accesses an HDI system file.[#] You can toggle the graph by selecting the check box in the bottom-right corner of the graph.</p> <p>Reads from the Primary HCP System</p> <p>Displays the number of times data has been recalled from the primary HCP.</p> <p>Reads from the Replica HCP System</p> <p>Displays the number of times data has been recalled from the replica HCP system.</p> <p>Error</p> <p>Displays the number of times that recall has failed.</p>
<p>[#]: In some cases, a recall is counted as having occurred at a slightly different time from when it actually occurred.</p>	

Shares tab

The **Shares** tab displays file share settings.

Table C-56 Items displayed in the Shares tab of the file-system-name window

Item	Description
Add button	<p>Displays the Add Share dialog box that can be used to add a file share (Add Share dialog box on page C-208).</p> <p>Note that a file share cannot be added if a read-write-content-sharing file system or home-directory-roaming file system and a file share have already been created.</p>
Edit button	<p>Displays the Edit Share dialog box that can be used to change the file sharing settings (Edit Share dialog box on page C-198).</p>
Release button	<p>Displays the Release Share(s) dialog box that can be used to release file shares (Release Share(s) dialog box on page C-204).</p>
Import Files button	<p>Displays the Import Files dialog box that can be used to import files from another file server (Import Files dialog box on page C-27).</p>

Item	Description
	You cannot import files from other file servers to file shares created in file systems that share data with other HDI systems via a linked HCP system.
Share Name	Displays share names.
Protocol	<p>Displays the protocol used for a file share.</p> <p>CIFS The CIFS protocol is used.</p> <p>NFS The NFS protocol is used.</p> <p>CIFS, NFS Both the CIFS and NFS protocols are used.</p>
Use Namespace	<p>Displays whether the HCP namespace is allocated to the share.</p> <p>If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.</p>
Content Sharing	<p>Displays how data is shared with other HDI systems via the linked HCP.</p> <p>Off Data is not being synchronized with other HDI systems.</p> <p>On (Read-Only) Data in other HDI systems is being referenced as read-only.</p> <p>If a file system is not linked to the HCP system at the share level, two hyphens (--) are displayed.</p>
File Share Capacity	<p>The value of the capacity of the migration-destination namespace is displayed in a bar graph. The ratio of the currently used capacity (%) is displayed inside the bar graph.</p> <p>If the share capacity is not limited based on the hard quota of the migration-destination namespace, two hyphens (--) are displayed.</p>
CIFS Share Name	<p>Displays CIFS share names. Clicking a CIFS share name displays the CIFS Protocol Settings dialog box (CIFS Protocol Settings dialog box on page C-197). If the CIFS protocol is not used, two hyphens (--) are displayed.</p>
Auto Creation of Home Directory	<p>Displays whether the function for automatically creating a home directory is used in the CIFS share. If the CIFS protocol is not used, two hyphens (--) are displayed.</p>
SMB Encryption	<p>Displays whether the communication with the CIFS client is to be encrypted when you use SMB 3.0.</p> <p>Auto Communication with the client is to be encrypted only when the client supports encryption.</p> <p>Mandatory</p>

Item	Description
	<p>Communication with the client is always to be encrypted.</p> <p>Disabled</p> <p>Communication with the client is not to be encrypted.</p> <p>Inherit CIFS service default</p> <p>The CIFS service configuration definitions are used.</p> <p>If the CIFS protocol is not used, two hyphens (--) are displayed.</p>
Export Point	<p>Displays the absolute path to the shared directory. Click the absolute path when the settings are specified to use the NFS protocol to display the NFS Protocol Settings dialog box (NFS Protocol Settings dialog box on page C-198).</p>
Target Namespace	<p>Displays the name of the namespace allocated to the share.</p> <p>To check the status of the migration-destination namespace, click <i>namespace-name</i> to display the <i>tenant-name</i> window (tenant-name window on page C-79).</p> <p>If the namespace is not allocated to the share, two hyphens (--) are displayed.</p>
External HCP Host Name	<p>Displays the host name or IP address that has been made external and is used to connect to the HCP system.</p> <p>If no host name or IP address is specified, two hyphens (--) are displayed.</p>
Namespace-access Account	<p>Displays the user name of the account used for viewing the migration-destination namespace.</p> <p>This item is displayed if data in other HDI systems is referenced as read-only or data is made available on other HDI systems via a linked HCP system at the share level.</p>
Replica System Name	<p>Displays the name of the replica HCP system.</p> <p>If no replica HCP system information is set, two hyphens (--) are displayed.</p>
External Replica HCP Host Name	<p>Displays the host name or IP address that has been made external and is used to connect to the replica HCP system.</p> <p>If no host name or IP address is specified, two hyphens (--) are displayed.</p>

Namespace tab

The **Namespace** tab displays namespace information for a linked HCP system.

Table C-57 Items displayed in the Namespace tab of the file-system-name window

Item		Description
Namespace Type		<p>Displays how the file system is linked to the HCP system.</p> <p>File System The file system is linked to the HCP system at the file system level.</p> <p>Subtree The file system is linked to the HCP system at the share level.</p>
Content Sharing		<p>Displays how data is shared with other HDI systems via the linked HCP.</p> <p>Off Data is not being synchronized with other HDI systems.</p> <p>On (Read-Only) Data in other HDI systems is being referenced as read-only.</p> <p>On (Read/Write) Data is being shared among HDI systems by using the read-write-content-sharing functionality (read-write-content-sharing file system).</p> <p>Home directory Roaming among HDI systems is enabled for home directory data created for each end user (home-directory-roaming file system).</p>
External HCP Host Name		<p>If data in another HDI system is referenced as read-only, the host name or IP address that has been made external and is used to connect to the HCP system is displayed.</p> <p>If no host name or IP address is specified, two hyphens (--) are displayed.</p>
Namespace-access Account	User	<p>Displays the user name of the account used for viewing the migration-destination namespace.</p> <p>This item is displayed if data in other HDI systems is referenced as read-only or data is made available on other HDI systems via a linked HCP system at the file system level.</p>
Task	Name	Displays the migration task name.
	Status	Displays the migration execution status.

Item		Description	
	Progress	Displays the progress of migration as a percentage (%).	
	Number of Errors	Displays the number of errors that occurred during migration.	
Migration Schedule	Start Date	Displays the first date on which migration is executed.	
	Regular Task Scheduling	Interval	Displays the interval at which migration is executed.
		Start Time	Displays the time at which migration starts.
		Maximum Duration	Displays how long migration processing is allowed to continue. If the value that is set is 0, the processing continues until all files are migrated.
Replica System Name		If data in another HDI system is referenced as read-only, the replica HCP system name is displayed.	
External Replica HCP Host Name		If data in another HDI system is referenced as read-only, the host name or IP address that has been made external and is used to connect to the replica HCP system is displayed. If no host name or IP address is specified, two hyphens (--) are displayed.	

Properties tab

The **Properties** tab displays settings such as WORM and the file version restore functionality.

Table C-58 Items displayed in the Properties tab of the file-system-name window

Item		Description	
WORM	Enabled	Displays whether the WORM settings are enabled.	
	Retention Period	Minimum	Displays the minimum retention period. If a period has not been set, <i>Infinite</i> is displayed.
		Maximum	Displays the maximum retention period. If a period has not been set, <i>Infinite</i> is displayed.
	Auto Commit	Enabled	Displays whether the autocommit settings are enabled.

Item		Description	
	Commit Mode	Displays the commit mode of autocommit. If autocommit processing is disabled, two hyphens (--) are displayed.	
	Time Until Committed	Displays the length of time before the next time autocommit processing will be executed. If autocommit processing is disabled, two hyphens (--) are displayed.	
	Default Retention Period	Displays the default retention period. If a default retention period has not been set, <i>Infinite</i> is displayed. If autocommit processing is disabled, two hyphens (--) are displayed.	
	Renaming of Empty Directories	Enabled Displays whether renaming empty directories is allowed in the WORM file system.	
Large File Transfer	Optimized	Displays whether the Large File Transfer function is used. This item is displayed if the version of linked HCP system is 8.0 or later.	
	Lower limit of the file size	Displays the lower threshold for the size of files to which the Large File Transfer function is applied. If the Large File Transfer function is not used, two hyphens (--) are displayed. This item is displayed if the version of linked HCP system is 8.0 or later.	
File Version Restore	In Use	Whether the past version files (past version directories) migrated to the HCP system are to be made available to clients is displayed.	
	Period to Hold	The period to keep the past version directories in the <code>.history</code> directory is displayed. This item is displayed if no custom schedule is used.	
	Custom Schedule	15-MINUTE Versions	The value specified for a custom schedule in 15-minute units is displayed (unit: minutes). If a custom schedule in 15-minute units is disabled, two hyphens (--) are displayed. This item is displayed if a custom schedule is used.
		HOURLY Versions	The value specified for an hourly custom schedule is displayed (unit: hours). If an hourly custom schedule is disabled, two hyphens (--) are displayed.

Item		Description
		This item is displayed if a custom schedule is used.
	DAILY Versions	The value specified for a daily custom schedule is displayed (unit: days). If a daily custom schedule is disabled, two hyphens (--) are displayed. This item is displayed if a custom schedule is used.
	WEEKLY Versions	The value specified for a weekly custom schedule is displayed (unit: weeks). If a weekly custom schedule is disabled, two hyphens (--) are displayed. This item is displayed if a custom schedule is used.
	MONTHLY Versions	The value specified for a monthly custom schedule is displayed (unit: months). If a monthly custom schedule is disabled, two hyphens (--) are displayed. This item is displayed if a custom schedule is used.
	YEARLY Versions	The value specified for a yearly custom schedule is displayed (unit: years). If a yearly custom schedule is disabled, two hyphens (--) are displayed. This item is displayed if a custom schedule is used.
CIFS Bypass Traverse Checking		Displays whether CIFS bypass traverse checking is enabled.
Cache Settings	Volume Group	Displays the name of the volume group used by the file system.
	Upper Limit at Expansion	Displays the upper limit for expansion of the file system capacity. If the initial capacity of a created file system is equal to or less than 32 GB, the maximum capacity after expansion will be less than the displayed value. For details about the initial capacity of a created file system and the maximum capacity after expansion, see the <i>CLI Administrator's Guide</i> .

Cache Resident Policy tab

The **Cache Resident Policy** tab displays policy information when cache resident policies are set up to prevent files from turning into stub files.

Table C-59 Items displayed in the Cache Resident Policy tab of the file-system-name window

Item		Description
Total Pinned Capacity		Displays the total capacity of pinned files.
Add button		Click to add a policy. Clicking this button displays the Add Cache Resident Policy dialog box (Add Cache Resident Policy dialog box on page C-237).
Edit button		Click to edit the conditions for a policy. Clicking this button displays the Edit Cache Resident Policy dialog box (Edit Cache Resident Policy dialog box on page C-237).
Delete button		Click to delete a policy. Clicking this button displays the Delete Cache Resident Policy dialog box (Delete Cache Resident Policy dialog box on page C-238).
Download List of Pinned Files button		Click to download a text file containing a list of pinned files.
Policy Name		Displays the policy name.
Directory		Displays the directory name.
File Types		Displays file type conditions.
File Size Range	Min	Displays minimum file size conditions.
	Max	Displays maximum file size conditions.
Comments		Displays comments about the policy.

Volume Groups window

The **Volume Groups** window displays the status of volume groups.

To display the **Volume Groups** window, select **Resources** in the top-left corner of the GUI, select the triangle icon next to *host-name* in the tree on the left side of the GUI, and then click **Volume Groups**.

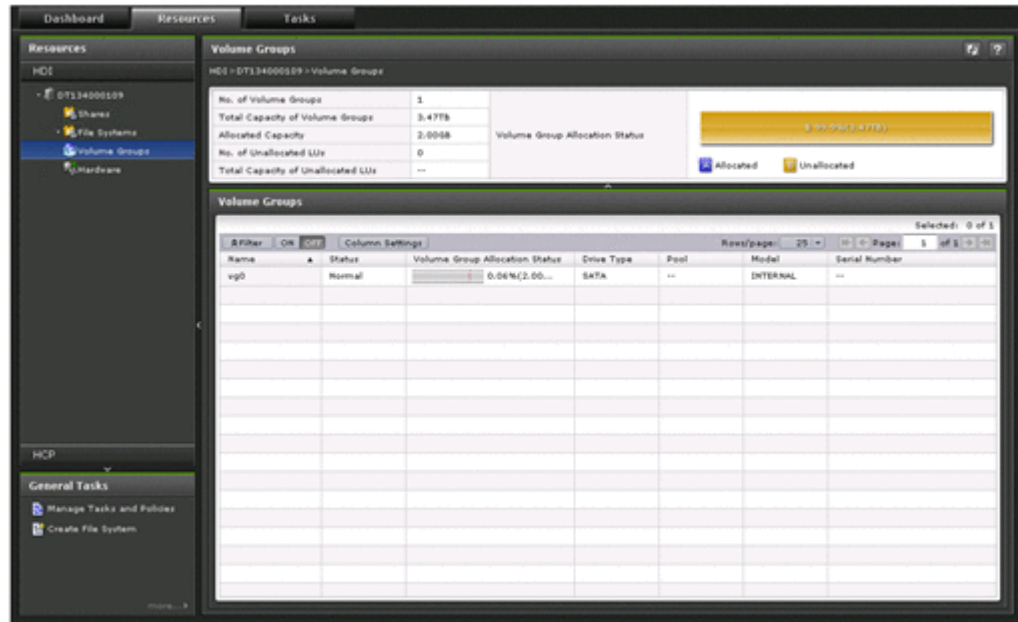


Table C-60 Items displayed in the Volume Groups window

Item		Description
No. of Volume Groups		Displays the total number of volume groups.
Total Capacity of Volume Groups		Displays the total capacity of all volume groups.
Allocated Capacity		Displays the total capacity of volume groups being used by file systems.
No. of Unallocated LUs		Displays the total number of internal hard disks and LUs in the storage system that have not yet been allocated to volume groups.
Total Capacity of Unallocated LUs		Displays the total capacity of internal hard disks and LUs in the storage system that have not yet been allocated to volume groups.
Volume Group Allocation Status		Displays the percentage (%) of the capacity allocated to the file systems, out of the total capacity of all volume groups.
Volume Groups area	Name	Displays the volume group names.
	Status	Displays the status of the volume groups.
	Volume Group Allocation Status	Displays the capacity currently allocated to the file systems and the capacity of the volume groups.
	Drive Type	Displays the drive type of the internal hard disks or LUs in the storage system that have been allocated to the volume groups. FC/SAS The drive type is FC, SAS, or SAS 7.2K for internal hard disks. SAS7K

Item	Description
	<p>The drive type is SAS 7.2K. SATA</p> <p>The drive type is SATA. SSD</p> <p>The drive type is SSD. Mixed</p> <p>Multiple drive types coexist. Also, -- is displayed if the LU is a virtual LU that uses Dynamic Tiering.</p>
Pool	<p>If virtual LUs for Dynamic Provisioning have been allocated to the volume group, the number of the pool to which the virtual LUs belong is displayed. If virtual LUs belong to multiple pools, <i>Mixed</i> is displayed.</p> <p>If no virtual LUs are allocated, -- is displayed.</p>
Model	<p>Displays the model of the storage system that contains the LUs allocated to the volume groups. For internal hard disks, <i>INTERNAL</i> is displayed.</p>
Serial Number	<p>Displays the serial number of the storage system that contains the LUs allocated to the volume groups. For internal hard disks, -- is displayed.</p>

Hardware window

The **Hardware** window displays the hardware and network statuses.

To display the **Hardware** window, select **Resources** in the top-left corner of the GUI, select the triangle icon next to a host name in the tree on the left side of the GUI, and then click **Hardware**.

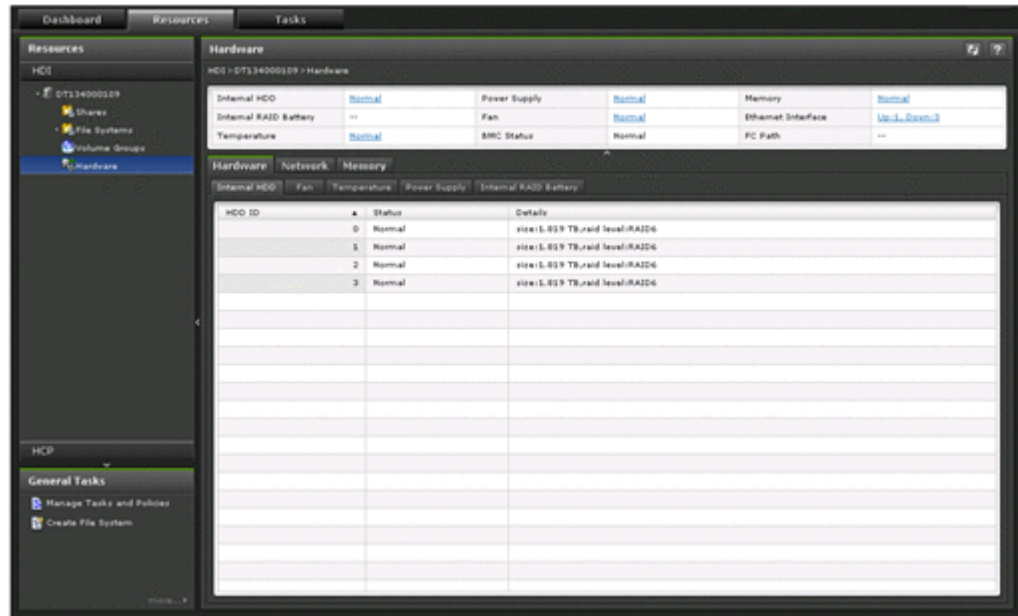


Table C-61 Items displayed in the Hardware window

Item	Description	See
Internal HDD	<p>Displays the status of internal hard disks.</p> <p>Normal</p> <p>All internal hard disks are running normally.</p> <p>Error</p> <p>Errors occurred for some internal hard disks. Take action according to the error information.</p> <p>--</p> <p>Information about internal hard disks cannot be obtained.</p>	--
Internal RAID Battery	<p>Displays the status of internal RAID batteries.</p> <p>Normal</p> <p>All internal RAID batteries are running normally.</p> <p>Error</p> <p>Errors occurred for some internal RAID batteries. Take action according to the error information.</p> <p>--</p> <p>Information about internal RAID batteries cannot be obtained.</p>	--
Temperature	<p>Displays results detected by temperature sensors.</p> <p>Normal</p>	--

Item	Description	See
	<p>All temperature sensors are detecting normal temperatures.</p> <p>Error</p> <p>Some temperature sensors detected abnormal temperatures. Take action according to the error information.</p> <p>--</p> <p>Information about temperature sensors cannot be obtained.</p>	
Power Supply	<p>Displays power unit statuses.</p> <p>Normal</p> <p>All power units are running normally.</p> <p>Error</p> <p>Errors occurred for some power units. Take action according to the error information.</p> <p>--</p> <p>Information about power units cannot be obtained.</p>	--
Fan	<p>Displays the fan status.</p> <p>Normal</p> <p>All fans are running normally.</p> <p>Error</p> <p>Errors occurred for some fans. Take action according to the error information.</p> <p>--</p> <p>Information about fans cannot be obtained.</p>	--
BMC Status	<p>Displays BMC statuses.</p> <p>Normal</p> <p>All BMCs are running normally.</p> <p>Error</p> <p>Errors occurred for some BMCs. Take action according to the error information.</p> <p>--</p> <p>Information about BMCs could not be obtained.</p>	--
Memory	<p>Displays the memory status.</p> <p>Normal</p> <p>All memory is running normally.</p> <p>Error</p>	--

Item	Description	See
	<p>Errors occurred for some memory. Take action according to the error information.</p> <p>--</p> <p>Information about memory cannot be obtained.</p>	
Ethernet Interface	<p>Displays the status of Ethernet interfaces (<i>ethn</i>, <i>mng0</i>, <i>pm0</i>, and <i>xgben</i>).</p> <p>The display format is as follows: <i>Up: number-of-ports-with-Up-link-status</i>, <i>Down: number-of-ports-with-Down-link-status</i></p>	--
FC Path	<p>Displays the FC path status if a storage system is to be connected. If no storage systems will be connected to, two hyphens (--) are displayed.</p>	--
Hardware tab	<p>Displays the hardware status for a node.</p>	Hardware tab on page C-75
Network tab	<p>Displays the network status.</p>	Network tab on page C-77
Memory tab	<p>Displays the memory information.</p>	Memory tab on page C-79

Hardware tab

The **Hardware** tab displays the hardware status for a node.

Table C-62 Items displayed in the Hardware tab of the Hardware window

Item	Description
Internal HDD tab	<p>Displays detailed information about the status of the internal hard disk.</p> <p>HDD ID</p> <p>Displays the ID of the internal hard disk.</p> <p>Status</p> <p>Displays the status of the internal hard disk.</p> <p><i>Normal</i>: The internal hard disk is running normally.</p> <p><i>Error</i>: An error has occurred for the internal hard disk.</p> <p><i>Rebuild</i>: The internal hard disk is currently being formatted or RAID is being constructed.</p> <p><i>Not supported</i>: The program that collects information has not been installed.</p> <p><i>Removed</i>: The internal hard disk was removed from the RAID group.</p> <p><i>Nodevice</i>: The internal hard disk was removed from the node.</p>

Item	Description
	<p>Setup: The internal hard disk installed on the node is not included in the RAID group.</p> <p>--: Information about the internal hard disk cannot be obtained.</p> <p>Details</p> <p>Displays information about the internal hard disk.</p>
Fan tab	<p>Displays detailed information about the status of the fan.</p> <p>Fan ID</p> <p>Displays the fan ID.</p> <p>Status</p> <p>Displays the fan status.</p> <p>Normal: The fan is running normally.</p> <p>Error: An error has occurred for the fan.</p> <p>--: Information about the fan cannot be obtained.</p> <p>Details</p> <p>Displays detailed information about the fan.</p>
Temperature tab	<p>Displays detailed information about the status of the temperature sensor.</p> <p>Sensor ID</p> <p>Displays the ID of the temperature sensor.</p> <p>Status</p> <p>Displays the status of the temperature sensor.</p> <p>Normal: The temperature sensor is running normally.</p> <p>Error: An error has occurred for the temperature sensor.</p> <p>--: Information about the temperature sensor cannot be obtained.</p> <p>Details</p> <p>Displays detailed information about the temperature sensor.</p>
Power Supply tab	<p>Displays detailed information about the status of the power unit.</p> <p>Power Supply ID</p> <p>Displays the ID of the power unit.</p> <p>Status</p> <p>Displays the status of the power unit.</p> <p>Normal: The power unit is running normally.</p> <p>Error: An error occurred for the power unit.</p> <p>Not installed: No power units are installed.</p> <p>--: Information about the power unit cannot be obtained.</p> <p>Details</p> <p>Displays detailed information about the power unit.</p>
Internal RAID Battery tab	<p>Displays detailed information about the internal RAID battery.</p> <p>Battery ID</p> <p>Displays the ID of the internal RAID battery.</p>

Item	Description
	<p>Status</p> <p>Displays the status of the internal RAID battery.</p> <p>Normal: The internal RAID battery is running normally.</p> <p>Error: Errors have occurred for some internal RAID batteries. Take action according to the error information.</p> <p>Charging: The internal RAID battery is charging.</p> <p>Not supported: The program that obtains information about the internal RAID battery is not installed.</p> <p>--: Information about the internal RAID battery cannot be obtained.</p> <p>Details</p> <p>Displays detailed information about internal RAID batteries.</p>

Network tab

The **Network** tab displays the network status.

Table C-63 Items displayed in the Network tab of the Hardware window

Item	Description
<p>Ethernet Interface tab</p>	<p>Displays detailed information about the Ethernet interface.</p> <p>Port Name</p> <p>Displays the port name of the Ethernet interface (<i>ethn</i>, <i>mng0</i>, <i>pm0</i>, or <i>xgben</i>).</p> <p>Type</p> <p>Displays the type of the port.</p> <p>Data LAN port: Displays <i>ethnumber</i> or <i>xgbenumber</i>. This port is used to access an HDI system from the front-end LAN.</p> <p>Management LAN port: Displays <i>mng0</i>. This port is used to access an HDI system from the front-end LAN.</p> <p>Private maintenance port: Displays <i>pm0</i>. This port is used for maintenance operations.</p> <p>Link Status</p> <p>Displays the status of the link.</p> <p>Up: The link is running normally.</p> <p>Down: The link has been disconnected. Check the negotiation mode of the switch connected to the port, and perform settings again.</p> <p>Media Type</p> <p>Displays the media type.</p> <p>Copper: Applies to metal cables.</p> <p>Fiber: Applies to optical cables.</p> <p>Link Speed</p> <p>Displays the LAN port transfer rate.</p>

Item	Description
	<p>10000Base: Communication is being performed at 10 Gbps.</p> <p>1000Base: Communication is being performed at 1 Gbps.</p> <p>100Base: Communication is being performed at 100 Mbps.</p> <p>10Base: Communication is being performed at 10 Mbps. Note that 10BASE is not a recommended transfer rate. Review the settings of the switch connected to the port to make sure the transfer rate is at least 100BASE.</p> <p>Unknown: Information about the transfer rate cannot be acquired.</p>
FC Path tab	<p>Displays detailed information about the FC path if a storage system has been connected.</p> <p>Path</p> <p>Displays the name of the FC path.</p> <p>Status</p> <p>Displays the status of the FC path.</p> <p>Online: The FC path is running normally.</p> <p>Online (LU error): While the status of the FC path was Online, an LU error was detected in the storage system.</p> <p>Offline: The FC path was placed in the offline status due to an operation of the system administrator.</p> <p>Offline (LU error): While the status of the FC path was Offline, an LU error was detected in the storage system.</p> <p>Partially online: The FC path is running normally, but some disks in the storage system cannot be accessed.</p> <p>Partially online (LU error): While the status of the FC path was Partially online, an LU error was detected in the storage system.</p> <p>Error: LUs in the storage system that belongs to the target FC path are not accessible.</p> <p>Configuration mismatch: Disk allocation to the host group associated with the FC path is different from the allocation for the alternate path, or there is no alternate path.</p> <p>Unknown: The FC path status cannot be checked.</p> <p>Target</p> <p>Displays the target.</p> <p>Model</p> <p>Displays the storage system model.</p> <p>Serial Number</p> <p>Displays the serial number of the storage system.</p> <p>Host Port</p> <p>Displays the name of the FC port on the node (host port).</p> <p>Host Port WWN</p> <p>Displays the WWN of the FC port on the node. If the FC port cannot be identified, two hyphens (--) are displayed.</p> <p>Array Port</p>

Item	Description
	<p>Displays the name of the FC port in the storage system.</p> <p>Array Port WWN</p> <p>Displays the WWN of the FC port in the storage system. If an error occurred in the FC path, two hyphens (--) are displayed.</p>

Memory tab

The **Memory** tab displays the memory information.

Table C-64 Items displayed in the Memory tab of the Hardware window

Item	Description
Memory Total tab	<p>Displays details about the memory size.</p> <p>Size</p> <p>Displays the memory size in the following format: <i>size:amount-of-memory-recognized-by-system</i></p>
Details tab	<p>Displays the detailed memory status information.</p> <p>Memory ID</p> <p>Displays the ID of a memory slot.</p> <p>Status</p> <p>Displays the memory status.</p> <p><i>Installed:</i> The memory is installed.</p> <p><i>Not installed:</i> No memory is installed.</p> <p><i>--:</i> The memory information cannot be obtained.</p> <p>Details</p> <p>The detailed memory information is displayed.</p>

tenant-name window

The *tenant-name* window displays tenant information for a linked HCP system.

To display the *tenant-name* window, select **Resources** in the top-left corner of the GUI, and then click **HCP** in the tree on the left side of the GUI.

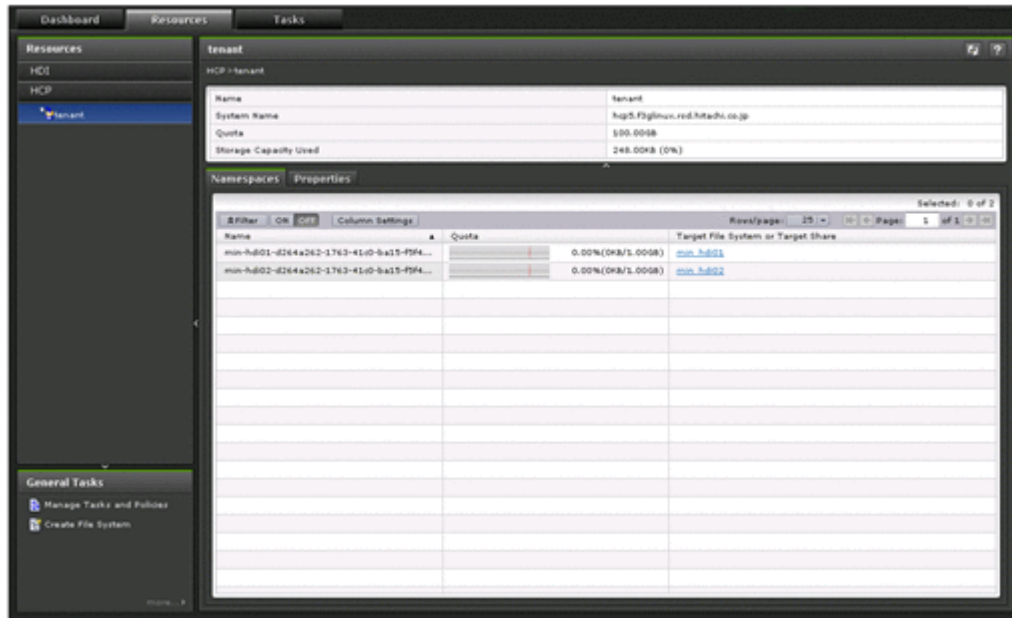


Table C-65 Items displayed in the tenant-name window

Item	Description	See
Name	Displays the tenant name.	--
System Name	Displays the HCP system name.	--
Quota	Displays the maximum capacity that can be used by the linked tenant.	--
Storage Capacity Used	Displays the current capacity used by the linked tenant and the percentage of the maximum capacity that the tenant can use.	--
Namespaces tab	Displays a list of migration-destination namespaces.	Namespaces tab on page C-80
Properties tab	Displays the tenant settings.	Properties tab on page C-81

Namespaces tab

The **Namespaces** tab displays the used capacity of a namespace and the name of a migration-source file system.

Table C-66 Items displayed in the Namespaces tab of the tenant-name window

Item	Description
Name	The name of the namespace.

Item	Description
Quota	Both the quota allocated to the namespace and the capacity currently being used.
Target File System or Target Share	The name of the file system or file share to which the namespace is allocated. If the namespace has not been allocated to the file system or file share, two hyphens (--) are displayed.

Properties tab

The **Properties** tab displays the information about the tenant administrator's user account and proxy server settings.

Table C-67 Items displayed in the Properties tab of the tenant-name window

Item	Description	
HCP Settings	Tenant Administrator	The user name of the migration-destination tenant administrator's user account.
	External HCP Host Name	The host name or IP address that has been made external and is used to connect to the HCP system. If no host name or IP address is specified, two hyphens (--) are displayed.
	Replica System Name	The replica HCP system name.
	External Replica HCP Host Name	The host name or IP address that has been made external and is used to connect to the replica HCP system. If no host name or IP address is specified, two hyphens (--) are displayed.
Proxy Server Settings	Host Name	The host name of the proxy server. If proxy server settings have not been completed, two hyphens (--) are displayed.
	Port	The port number used for the proxy server. If proxy server settings have not been completed, two hyphens (--) are displayed.
	User Name	The user name used for proxy server authentication. If proxy server settings have not been completed, two hyphens (--) are displayed.

Import Files window

In the **Import Files** window, you can check the status of files being imported from another file server.

To display the **Import Files** window, choose **Tasks** in the top-left corner of the GUI.

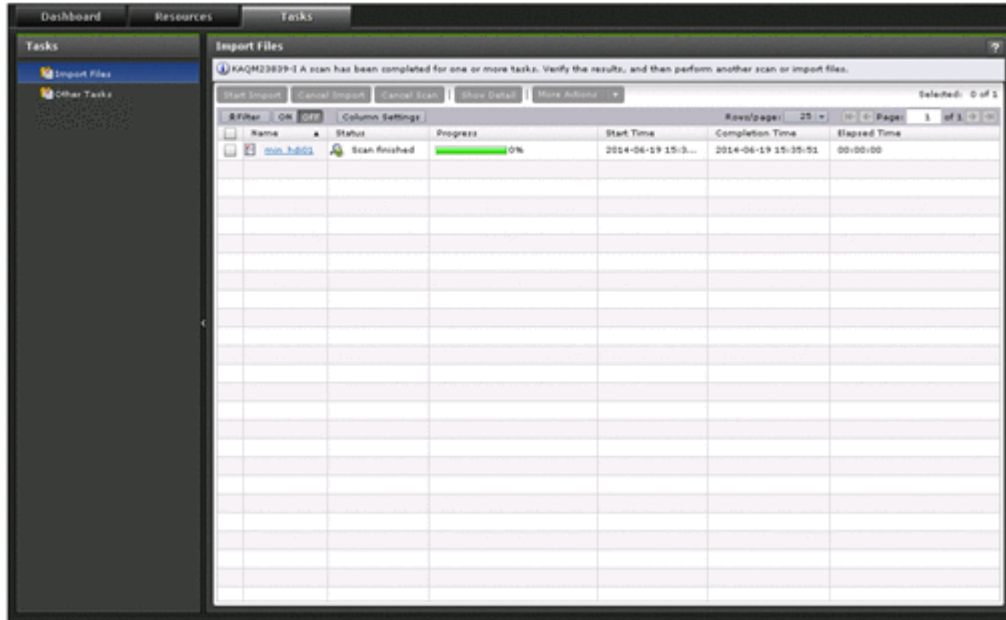


Table C-68 Items displayed in the Import Files window

Item	Description
Start Import button	Starts the importing of files. This button becomes active after verification of files finishes. Clicking this button displays a confirmation dialog box (Table C-69 Items displayed in the confirmation dialog box for task operations on page C-83).
Cancel Import button	Stops the importing of files. Clicking this button displays a confirmation dialog box (Table C-69 Items displayed in the confirmation dialog box for task operations on page C-83).
Cancel Scan button	Stops the verification of files. Clicking this button displays a confirmation dialog box (Table C-69 Items displayed in the confirmation dialog box for task operations on page C-83).
Show Detail button	Checks the details about the task. Clicking this button displays the Import Files dialog box (Import Files dialog box on page C-27).
More Actions	Click <input type="checkbox"/> and perform the necessary operation. Change to On-Demand Import Changes the import method to on-demand importing. If you click this button to change the import method, only the source files that are requested by a client are imported when the client accesses the files. Clone Task Defines a task that has the same settings as the selected task. Delete Task

Item	Description
	Deletes the selected tasks.
Name	Displays the task names. Clicking a task name displays the Import Files dialog box (Import Files dialog box on page C-27).
Status	<p>Displays the current status of the task.</p> <p>Importing</p> <p>Files are being imported.</p> <p>Importing(Temporary On-Demand)</p> <p>The import method has been changed to on-demand importing because a migration to the HCP system was started or the free file system capacity on the import target reached the threshold.</p> <p>Import finished</p> <p>Importing files finished.</p> <p>Import stopped</p> <p>The importing of files from another file server was stopped.</p> <p>Maintenance required</p> <p>An error occurred. Check the details about the error, and take actions for recovery.</p> <p>On-demand</p> <p>Only the files accessed by clients are imported on demand.</p> <p>Scanning</p> <p>Whether the files can be imported is being verified.</p> <p>Scan finished</p> <p>Verification of the files finished.</p> <p>Scan stopped</p> <p>Verification of the files was stopped.</p>
Progress	Displays the progress of the task.
Start Time	Displays the date and time the verification or importing of files started.
Completion Time	Displays the date and time the verification or importing of files finished.
Elapsed Time	Displays the time elapsed since the verification or importing of files started.

Table C-69 Items displayed in the confirmation dialog box for task operations

Item	Description
Name	Displays the name of the selected task.
Source Host	Displays the name of the host specified as the import source for the task.
Source Share	Displays the name of the shared directory specified as the import source for the task.

Item	Description
Target Host	Displays the HDI node specified as the import target of files for the task.
Target Share	Displays the name of the shared directory of the HDI specified as the import target of files for the task.
Apply button	Execute the operation.

Restart Node dialog box

You can restart a node.

To display the **Restart Node** dialog box, click the **Restart Node** button in the *host-name* window.



Note: If encryption of local data is enabled, when you save system settings to the HCP system, confirm that the HCP system is running normally and that the HDI and HCP systems can communicate normally before restarting the node.

Table C-70 Items displayed in the Restart Node dialog box

Item		Description
Node Information	Host Name	The name of the host on the node
	Node status	The node status. Online The node is operating normally. Online Pending The node is being started. Offline The node is not running. Offline Pending The node is being stopped. Partial Online Some services are not running. Error An error has occurred. See the error information, and take appropriate action.
	IP Address (mng0)	The IP address
Yes, I have read the above warning. check box		Select this check box if you want to restart the node.
Apply button		Restarts the node. The Yes, I have read the above warning. check box must be selected before you click this button.

System Software Installation dialog box

You can update the software running on the node. You can also check whether the latest software has been installed.

To display the **System Software Installation** dialog box, click **Software Update** in the **Settings** area of the *host-name* window.

Table C-71 Items displayed on the System Software Installation dialog box

Item		Description
Product name		Displays the name of the installed product.
Current version		Displays the version of the software that is currently installed.
Backup Configuration button		Saves the system configuration information before installing the software. Click this button to display the Backup Configuration dialog box (Backup Configuration dialog box on page C-97). This button appears when the HCP Anywhere is not linked.
Available Versions	System Version	Displays a list of the software versions that can be installed.
I want to update the system software. or Yes, I backed up the system settings and wish to update the system software. check box		Checks information before installing the software.
Install button		Installs the software. Select the software version that you want to install, select I want to update the system software. or Yes, I backed up the system settings and wish to update the system software. , and then click this button.

Local Users dialog box

You can manage information about the users who can access a file system.

To display the **Local Users** dialog box, click **Local Users** in the **Settings** area of the *host-name* window.

List of Users / Groups page

You can view the information about the users registered in an HDI system and the groups containing users.

The **List of Users / Groups** page appears first when the **Local Users** dialog box is displayed.

Table C-72 Items displayed on the on the List of Users / Groups page

Item	Description
Drop-down list	Select the information to be displayed. List of users: Display user information. List of groups: Display group information.
Display button	Displays information.

**Table C-73 User information displayed in the List of Users / Groups page
(for List of users)**

Item	Description
User name	Displays the user name.
UID	Displays the user ID.
GID	Displays the ID of the primary group to which the user belongs.
Comment	Displays comments about the user. This item is not displayed unless a comment has been specified.

**Table C-74 Group information displayed in the List of Users / Groups page
(for List of groups)**

Item	Description
Group name	Displays the group name.
GID	Displays the group ID.

**Table C-75 Operations that can be performed for a user on the List of
Users / Groups page (for List of users)**

Buttons	Description	See
Change Password button	Changes the password for the user selected by the radio button.	Change Password page on page C-87
Edit User button	Edit the information for the user selected by the radio button.	Edit User page on page C-87
Delete User button	Deletes the information for the user selected by the radio button. Batch registered users can also be deleted.	-
Add New User button	Adds a user.	Add User page on page C-88
Batch Operation button	Registers or deletes multiple user information in a batch operation.	Batch Operation page on page C-89
Legend: -: Not applicable		

Table C-76 Operations that can be performed for a group on the List of Users / Groups page (for List of groups)

Buttons	Description	See
Edit Group button	Edits the information for the group selected by the radio button.	Edit Group page on page C-95
Delete Group button	Deletes the information for the group selected by the radio button.	-
Add New Group button	Adds a group.	Add Group page on page C-96
Legend: -: Not applicable		

Change Password page

You can change the password of a user.

To display the **Change Password** page, select **List of users** from the drop-down list on the **List of Users / Groups** page, click the **Display** button, select the user, and then click the **Change Password** button.

Table C-77 Items displayed on the Change Password page

Item	Description
User name	Displays the user name whose password you want to change.
New password	Enter the new password.
Re-enter new password	Re-enter the password you set in New password .

Edit User page

You can edit user information.

To display the **Edit User** page, select **List of users** from the drop-down list on the **List of Users / Groups** page, click the **Display** button, select the user, and then click the **Edit User** button.



Note: Items whose information is not changed retain their current settings.

Table C-78 Items displayed on the Edit User page

Item	Description
User name	Displays the user name.
UID	Displays the user ID.
GID	Change the ID of the primary group to which the user belongs.

Item	Description
Comment	Change the comment for the user. This item is optional.
Applied to CIFS environment	Displays whether the user is permitted to access CIFS shares.
Groups	Change the groups to which the user belongs. Up to 32 groups can be specified per user. However, if a user belongs to more than 16 groups and is using UNIX (AUTH_SYS) authentication for when they access NFS file shares, they will only be granted access permission for the first 16 groups. <ul style="list-style-type: none"> To add groups to the user: In List of selectable groups, select the groups you want to add to the user, and then click the ▼ button. You can add only the groups displayed in Selected groups. To delete groups from the user: In Selected groups, select the groups you want to delete from the user, and then click the ▲ button.

Add User page

A system administrator can add a user.

To display the **Add User** page, select **List of users** from the drop-down list on the **List of Users / Groups** page, click the **Display** button, and then click the **Add New User** button.



Note:

- The groups that include the users to be added must be registered beforehand.
- Make sure that the number of users is not more than 2,000.

Table C-79 Items displayed on the Add User page

Item	Description
User name	Enter the user name. You cannot specify a user name that has already been registered in the HDI system, on the NIS server, or on the LDAP server for user authentication. To add the user as a user of CIFS shares, you cannot specify a name that is the same as that of an existing group configured to use the ACL functionality. Enter a maximum of 16 characters. The first character must be an alphanumeric character. You can use any alphanumeric character, hyphen (-), and underscore (_) after the first character. In Windows, the entered value is not case sensitive. Specify a name that is unique regardless of whether upper-case or lower-case alphabetic characters are used.

Item	Description
	Also, you cannot specify the user name already shown in Table E-2 List of reserved words for the user name on page E-2 because the user name is reserved by the OS.
UID	Enter the user ID. Specify a value from 200 to 2147483147. You cannot specify 65534 or the user ID that has already been registered in the HDI system, on the NIS server, or on the LDAP server for user authentication. In addition, when user mapping is being used, you cannot specify the user IDs within the ID range set by user mapping.
GID	Specify the ID of the primary group to which the user belongs.
Password	Enter the user password, using from 6 to 20 characters. You can specify alphanumeric characters and the following symbols: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~
Re-enter password	Re-enter the password you set in Password .
Comment	Enter a comment for the user. Use a maximum of 32 characters. You can specify alphanumeric characters and the following symbols: # % & ' () * + - . / ; < > ? @ [] ^ _ { } ~ You can also specify spaces, but not at the beginning or end of the character string. This item is optional. When the user uses CIFS shares, this comment is used for displaying ACLs.
Apply to CIFS environment	Select this check box when you want to add the user as a user of CIFS shares.
Groups	Specify groups to which the user belongs. Select, in List of selectable groups , the groups you want to add to the user, and then click the ▼ button. You can add only groups that are displayed in Selected groups . Up to 32 groups can be specified per user. However, if a user belongs to more than 16 groups and is using UNIX (AUTH_SYS) authentication for when they access NFS file shares, they will only be granted access permission for the first 16 groups. To delete groups from a user, select the user in Selected users , and then click the ▲ button.

Batch Operation page

Use a CSV file containing user information to register or delete information about multiple users in a batch operation.



Note:

- Prepare the CSV file containing user information in advance. For details about the CSV file format, see [CSV file format on page C-90](#).

- The password information, which is provided for users who are to be registered, is also contained in the CSV file, so manage the file carefully.
- Depending on the number of users whose information is to be registered or deleted, several tens of minutes might be required to finish the operation.

To display the **Batch Operation** page, select **List of users** from the drop-down list on the **List of Users / Groups** page, click **Display**, and then click **Batch Operation**.

Table C-80 Items displayed on the Batch Operation page

Item	Description
Name of batch configuration file	Specify the path to the CSV file containing user information. To view the file name to specify the path, click the Browse button.
Check and Register button	Check the CSV file format, and then register or delete user information in a batch operation. If there are no errors in the CSV file, user information is registered or deleted in a batch operation. If an error is found, none of the user information is registered or deleted.
Check File button	Only check the CSV file format.

When the check is completed, you can download the execution result file containing the check results. Check the execution results file and, if an error is found, take corrective action.

For details about the error and the action to be taken, see [Table C-82 Error messages, error causes, and actions when an error occurs during batch registration of user information on page C-92](#) or [Table C-83 Error messages, error causes, and actions when an error occurs during batch deletion of user information on page C-94](#).

CSV file format

You can use any alphanumeric characters, hyphens (-), underscores (_), and periods (.) in the file name. Also make sure that the path name of a CSV file specified on the **Batch Operation** page does not contain more than 512 characters.

Table C-81 Information specified in a CSV file for batch registration or batch deletion of user information

Item	When registering	When deleting	Description
Execution category	R	R	Specify the execution category of the data (Data).

Item	When registering	When deleting	Description
Data classification	R	R	The processing classification of the data. Note that UA01 and UD01 cannot exist within the same file. UA01 Batch-register the data. UD01 Batch-delete the data.
Data registration destination	R	R	To register user information: Specify where the user information is to be registered or reflected. 1 Register in the HDI system. 3 Register the users in the HDI system as users who access CIFS shares. To delete user information: Use the information directly below this table to create a CSV file for deleting user information.
User name	R	R	Specify the user name. The values that can be specified are the same as those that can be specified in User name , in the Add User page.
UID	R	N/R	Specify the user ID. The values that can be specified are the same as those that can be specified in UID , in the Add User page.
GID	R	N/R	Specify the ID of the primary group to which the user belongs.
Password	R	N/R	Specify the user password. The values that can be specified are the same as those that can be specified in Password , in the Add User page.
Comment	I	N/R	Specify a comment for the user. The values that can be specified are the same as those that can be specified in Comment , in the Add User page.
Groups	I	N/R	Use a group name or group ID to specify the other groups to which the user belongs. Use commas (,) to delimit multiple group names or group IDs, and enclose the entire string with double quotation marks (").
Legend: R: Required. I: If necessary. N/R: Not required.			

Example of batch registration

```
#execution-category,data-classification,data-registration-destination,user-  
name,UID,GID,password,comment,groups  
Data,UA01,3,username,205,205,password,fullname,"206,207,208"
```

Example of batch deletion

```
#execution-category,data-classification,,user-name  
Data,UD01,,username
```

Execution results file format

Example when a CSV file check is only performed and no errors are found

OK is output to the execution category of the user.

```
#execution-category,data-classification,data-registration-destination,user-  
name,UID,GID,password,comment,groups  
OK,UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

Example when batch registration or deletion is performed normally

#Completed is output to the execution category of the user

```
#execution-category,data-classification,data-registration-destination,user-  
name,UID,GID,password,comment,groups  
#Completed,UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

Example when the CSV file contains an error

NG (*error-message*) is output to the execution category for the user.

```
#execution-category,data-classification,data-registration-destination,user-  
name,UID,GID,password,comment,groups  
NG(The specified UID is already  
registered),UA01,3,user04,1004,1000,password,Leader,"unit01,2000"
```

Table C-82 Error messages, error causes, and actions when an error occurs during batch registration of user information

Error message	Error cause	Action
The group to which the user belongs is incorrect	The group name or group ID specified in the Groups could not be found.	Check the Groups.
The comment is invalid	The comment is incorrect. The value might contain a character that cannot be used or the value length might be incorrect.	Check the comment.

Error message	Error cause	Action
The data classification value is invalid	The value specified in the process category is incorrect.	Check the value specified in the process category. Specify UA01 in the process category.
The value for the data registration destination is invalid	The data registration destination value is incorrect.	Check the data registration destination value. Specify 1 or 3 in the data registration destination value.
The execution classification value is invalid	The value specified in the execution category is incorrect.	Check the value specified in the execution category. Specify Data or hash mark (#) in the execution category.
The GID value is invalid	The group ID value is incorrect or a group with the specified group ID cannot be found. The value might contain a character that cannot be used or specified value is outside the valid range.	Check the group ID. The valid range of the value is from 200 to 2147483147. However, you cannot use 65534.
The number of elements is invalid	The number of elements for batch registration specified in the CSV file is incorrect.	Check the number of elements for batch registration. The number of elements for batch registration is from 7 to 9.
An invalid character is specified in the password	The specified password is incorrect. The password might contain a character that cannot be used or the value length might be incorrect.	Check the password.
The UID is duplicated in the CSV file	The same user ID exists in the CSV file.	Check the user ID.
The user name is duplicated in the CSV file	The same user name exists in the CSV file.	Check the user name.
The specified UID is already registered	The specified user ID has already been registered.	Check the user ID.
The specified user is already registered	The specified user name has already been registered.	Check the user name.
The UID value is invalid	The user ID value is incorrect. The value might contain a character that cannot be used or specified value is outside the valid range.	Check the user ID. The valid range of the value is from 200 to 2147483147. However, you cannot use 65534.

Error message	Error cause	Action
The user name value is invalid	The user name value is incorrect. The value might contain a character that cannot be used or the value length might be incorrect.	Check the correct user name.
The specified user name is already specified for a group name registered in the CIFS ACL environment	The specified user name is the same as the group name registered in the CIFS (ACL) environment.	Specify another user name.
An attempt to acquire a locked resource failed	An internal error occurred. <ul style="list-style-type: none"> You could not obtain an exclusive resource (a timeout occurred). 	Re-execute batch registration of the user information. If the error occurs again, download all of the log files on the node and then contact maintenance personnel.
Registration failed	An internal error occurred. <ul style="list-style-type: none"> You could not obtain an exclusive resource (a timeout does not cause the error). The group ID of the group to which the user belongs could not be converted into the group name (file operations might fail or group information might not exist). The user registration command failed. 	Re-execute batch registration of the user information. If the error occurs again, download all of the log files on the node and then contact maintenance personnel.

Table C-83 Error messages, error causes, and actions when an error occurs during batch deletion of user information

Error message	Error cause	Action
The data classification value is invalid	The value specified in the process category is incorrect.	Check the value specified in the process category. Specify UD01 in the process category.
The execution classification value is invalid	The value specified in the execution category is incorrect.	Check the value specified in the execution category. Specify Data or hash mark (#) in the execution category.
The number of elements is invalid	The number of elements for batch deletion specified in the CSV file is incorrect.	Check the number of elements for batch deletion.

Error message	Error cause	Action
		For batch deletion of user information, assume four elements as shown below: #execution-category,data-classification,,user-name Data,UD01,,username
The user name is duplicated in the CSV file	The same user name exists in the CSV file.	Check the user name.
The specified user does not exist	The specified user name has not been registered.	Check the user name.
The user name value is invalid	The user name value is incorrect. The value might contain a character that cannot be used or the value length might be incorrect.	Check the user name.
An attempt to acquire a locked resource failed	An internal error occurred. <ul style="list-style-type: none"> You could not obtain an exclusive resource (a timeout occurred). 	Re-execute batch deletion of user information. If the error occurs again, download all of the log files on the node and then contact maintenance personnel.
Deletion failed	An internal error occurred. <ul style="list-style-type: none"> The user deletion command failed. You could not obtain an exclusive resource (a timeout does not cause the error). 	Re-execute batch deletion of user information. If the error occurs again, download all of the log files on the node and then contact maintenance personnel.

Edit Group page

A system administrator can edit information of a group in **Edit Group** page.

To display the **Edit Group** page, select **List of groups** from the drop-down list on the **List of Users / Groups** page, click **Display**, select the target group, and then click **Edit Group**.



Note: Items whose information is not changed retain their current settings.

Table C-84 Items displayed on the Edit Group page

Item	Description
Group name	Specify a new group name. You cannot change the group name if Yes is displayed for Applied to CIFS ACL environment .

Item	Description
GID	Displays the group ID.
Applied to CIFS ACL environment	Displays whether ACLs are set for the group.
Users in group	<p>Change the users who belong to the group.</p> <ul style="list-style-type: none"> To add users to the group: In List of selectable users, select the users you want to add, and then click the ▼ button. You can select only the users displayed in Selected users. To delete users from the group: In Selected users, select the users you want to delete, and then click the ▲ button.

Add Group page

A system administrator can add a group in **Add Group** page.

To display the **Add Group** page, select **List of groups** from the drop-down list on the **List of Users / Groups** page, click **Display**, and then click **Add New Group**.



Note: Make sure that the number of groups is not more than 2,000.

Table C-85 Items displayed in the Add Group page

Item	Description
Group name	<p>Enter the group name.</p> <p>You cannot enter any group name that has already been registered in the HDI system, on the NIS server, or on the LDAP server for user authentication.</p> <p>Enter a maximum of 16 characters. The first character must be an alphanumeric character. You can use any alphanumeric character, hyphen (-), and underscore (_) after the first character.</p> <p>In Windows, the entered value is not case sensitive. Specify a name that is unique regardless of whether upper-case or lower-case alphabetic characters are used.</p> <p>If ACL functionality is to be used for the group being added, you cannot specify a name that is the same as that of any user configured to access CIFS shares.</p> <p>Also, you cannot specify the group name shown in Table E-3 List of reserved words for the group name on page E-3 because the group name is reserved by the OS.</p>
GID	<p>Enter the group ID.</p> <p>Specify a value from 200 to 2147483147. You cannot specify 65534 or the group ID that has already been registered in the HDI system, on the NIS server, or on the LDAP server for user authentication. In</p>

Item	Description
	addition, when user mapping is being used, you cannot specify the group IDs within the ID range set by user mapping.
Apply to CIFS ACL environment	Select this check box when setting an ACL for the adding group.
Users in group	<p>Specify the users you want to add to the group.</p> <p>In List of selectable users, select the users you want to add to the group, and then click the ▼ button. You can add only the users displayed in Selected users.</p> <p>To delete users from the group, in Selected users, select the users you want to delete, and then click the ▲ button.</p>

Backup Configuration dialog box

You can download the system configuration file (the file in which system configuration information is archived) and save it in storage media outside the system, and upload the downloaded system configuration file if an error occurs.



Note:

- If the system configuration file (the file in which system configuration information is archived) is not downloaded, you might not be able to properly restore the system after a failure occurs in a system disk or storage system. Therefore, download the system configuration file, and then save the file to storage media outside of the system.
- If the periodic saving of system configuration information is enabled and you change the system configuration, you need to manually save the system configuration information and download the system configuration information file.
- If an error occurs while periodic saving of system configuration information is enabled, and you can still display the **Backup Configuration** dialog box, disable periodic saving. Periodic saving might overwrite correct data with incorrect data generated after the failure.
- The system configuration information file contains password information for system administrators, end users, and administrators of external servers. Be especially careful when managing a downloaded system configuration information file.
- The system administrator cannot edit a downloaded system configuration file. In addition, the system configuration file cannot be used in a different system version of the HDI system.
- Make sure that you set the time for periodic saving to a time period during which no jobs of the NDMP functionality are running. In addition, make sure that you do not execute a command or use the GUI at the time when periodic saving is performed.

To display the **Backup Configuration** dialog box, click **Backup Configuration** in the **Settings** area of the *host-name* window.

Save System Settings Menu page

You can download the system configuration information file, and upload the system configuration information file that has been downloaded.

The **Save System Settings Menu** page appears first when the **Backup Configuration** dialog box is displayed.

Table C-86 Items displayed on the Save System Settings Menu page

Buttons	Description	See
Save All System Settings button	Saves system configuration information and downloads the system configuration information file. Settings related to periodic saving can also be specified.	Save All System Settings page on page C-98
Upload Saved Data button	Upload the system configuration information file on the node according to the instructions from maintenance personnel, or delete the uploaded file from the node.	Upload Saved Data page on page C-102

Save All System Settings page

You can download the system configuration information file.



Note: It takes about 4 minutes to save the system configuration information. When there is a heavy load on a node, a save operation for the system disk might automatically stop to reduce the load on the node (The processing of OS disks times out after about 5 minutes from the start of the save processing.). In this case, after the load on the node is reduced and stabilized, retry the save operation.

To display the **Save All System Settings** page, click the **Save All System Settings** button on the **Save System Settings Menu** page.

Table C-87 Items displayed on the Save All System Settings page

Item	Description
Save status	<p>Status</p> <p>Displays the save and restore status of the system configuration information.</p> <p>Normal</p> <p>The processing to save or restore the system configuration information has completed.</p> <p>Now saving...</p> <p>The system configuration information is being saved.</p> <p>Now restoring...</p>

Item	Description
	<p>The system configuration information is being restored.</p> <p>Do not attempt to save or download the file if the displayed status is not <code>Normal</code>.</p>
	<p>Last save date</p> <p>Displays the date and time when the system configuration information was last saved. If no data has been saved, a hyphen (-) is displayed.</p>
<p>Save schedule</p>	<p>Schedule setting status</p> <p>Displays whether the periodic saving of system configuration information is enabled.</p> <p>On</p> <p>Periodic saving is enabled.</p> <p>Off</p> <p>Periodic saving is disabled.</p>
	<p>Schedule interval</p> <p>Displays the interval at which the periodic saving of system configuration information is executed.</p> <p>Daily</p> <p>Periodic saving is executed every day.</p> <p>Weekly</p> <p>Periodic saving is executed on the specified day of the week. The specified day of the week is also displayed.</p> <p>Monthly</p> <p>Periodic saving is executed on the specified date every month. The specified date is also displayed.</p>
	<p>Schedule time</p> <p>Displays the time that the periodic saving of system configuration information starts.</p>
	<p>Output setting</p> <p>Displays the location in which the system configuration information file will be saved when periodic saving is executed.</p> <p>Server transfer (HCP)</p> <p>The system configuration information file will be saved in the HCP system.</p> <p>Server transfer (FTP)</p> <p>The system configuration information file will be transferred to the FTP server.</p> <p><i>directory-path</i></p> <p>The system configuration information file will be saved in the displayed directory in the home directory or file system.</p> <p>If the system configuration information file is not to be output, a hyphen (-) is displayed.</p>
	<p>FTP server</p> <p>Displays the IP address or host name of the FTP server to which the system configuration information file is to be transferred when the</p>

Item	Description
	periodic saving of system configuration information is executed. If no information has been set, a hyphen (-) is displayed.
User name	Displays the name of the user who logs on to the FTP server for the periodic saving of system configuration information. If no information has been set, a hyphen (-) is displayed.
Directory	Displays the directory on the FTP server to which the system configuration information file is to be transferred when the periodic saving of system configuration information is executed. If no information has been set, a hyphen (-) is displayed.
Download button	Downloads the system configuration information.
Enable Scheduling button or Disable Scheduling button	Enables or disables the periodic saving of system configuration information. You can check the settings in Schedule setting status on the Save All System Settings page.
Modify Schedule button	Sets the periodic saving interval for system configuration information. The Schedule Settings for Saving All System Settings page is displayed (Schedule Settings for Saving All System Settings page on page C-100).

Schedule Settings for Saving All System Settings page

You can set the periodic saving interval for system configuration information.



Note: Saving system configuration information imposes heavy loads on the node. When specifying a date and time for an interval for periodic saving, avoid time periods during which you expect heavy access to the node (such as when the system administrator performs maintenance tasks or when end users use file systems).

In addition, we recommend that you avoid periods that will include the switchover date for daylight saving time when specifying the start time of periodic saving. If periodic saving is executed on the switchover date for daylight saving time, data might not be saved or might be saved twice.

To display the **Schedule Settings for Saving All System Settings** page, click **Modify Schedule** on the **Save All System Settings** page.

Table C-88 Items displayed on the Schedule Settings for Saving All System Settings page

Item	Description
Interval	<p>The interval in which periodic saving of system configuration information is executed. Select an option.</p> <p>Daily Periodic saving is executed every day.</p> <p>Weekly Periodic saving is executed on the specified day of the week. Select the check box to specify the day of the week when periodic saving is to be executed.</p> <p>Monthly Periodic saving is executed on the specified date every month. Select the check box to specify the date when periodic saving is to be executed. Periodic saving is not executed on a date that does not exist for a given month. (Example: the 31st day of February)</p>
Time	<p>The time when periodic saving starts. You can specify the time in one-minute units, in the range from 00:00 to 23:59.</p>
Output setting	<p>Specify the directory to which the system configuration file is to be saved.</p> <p>Note that If you select a value other than Output to home directory, the system settings file is also saved immediately under the SSH account's home directory (<code>/home/nasroot</code>).</p> <p>Transfer to HCP Select to save the system configuration file in an HCP system.</p> <p>Output directory Select to save the system configuration file in a file system. In the text box, specify the directory to save the system configuration file in. Make sure that you specify an absolute path that begins with <code>/mnt/#</code>. If you click Select, the List of Mounted File Systems page is shown. Select the target file system.</p> <p>Output to home directory Select to save the system configuration file in the home directory for SSH account (<code>/home/nasroot</code>).</p> <p>Transfer to FTP server Select to transfer the system configuration file to the FTP server. If you select this item, also specify the following information: FTP server: Specify the IP address or host name of the FTP server. We recommend that you specify the IP address. User name: Specify the name of the user who logs on to the FTP server. Password: Specify the password of the user. Directory: Specify the transfer-destination directory. Note that you cannot specify a character string that includes double</p>

Item	Description
	quotation marks ("), dollar sign (\$), asterisk (*), grave accent mark (`), space, and non-ASCII characters. You cannot, however, use a backslash (\) as the last character. Create the directory in the FTP server before you transfer the file.
	<p>#: Specify a directory in a file system that is mounted with reading and writing allowed. Note that the following directories cannot be specified:</p> <ul style="list-style-type: none"> • A directory whose path contains a symbolic link • A directory in a file system that shares data with other HDI systems via the linked HCP • A directory whose path contains any of the following directories: .conflict, .conflict_longpath, .history, .snaps, .lost+found • A directory in the root directory of a file system and with any of the following names: .arc, .system_gi, .system_reorganize, and lost+found

List of Mounted File Systems page

You can select a file system to which the system configuration file is saved.

To display the **List of Mounted File Systems** page, on the **Schedule Settings for Saving All System Settings** page, click the **Select** button for **Output directory**.

Table C-89 Items displayed on the List of Mounted File Systems page

Item	Description
File system	Displays the file systems mounted with reading and writing allowed.
Mount point	Displays the mount point for the file system.

Upload Saved Data page

You can upload the system configuration information file on a node.



Note: To restore other settings that were changed after downloading, perform the same setup procedure again after restoring data to the system disk.

To display the **Upload Saved Data** page, click the **Upload Saved Data** button on the **Save System Settings Menu** page.

Table C-90 Items displayed on the Upload Saved Data page

Item	Description
Name of saved file	Displays the name of the system configuration file if the file has already been uploaded.

Item	Description
	If the file has not been uploaded, a hyphen (-) is displayed.
Available OS disk space (KB)	Displays the amount of free space in the OS disk. If there is no free space, or the information about space cannot be acquired, a hyphen (-) is displayed.
Upload button	Specifies the system configuration information file to be uploaded to the node. Clicking this button displays the Select Saved Data File page. In Saved file , use an absolute path to specify the system configuration information file to be uploaded.
Delete button	Deletes the system configuration information file uploaded to the node. Note: You cannot delete a system configuration information file that was transferred using the <code>scp</code> command. For details about how to delete system configuration information files transferred using the <code>scp</code> command, see the <i>CLI Administrator's Guide</i> .

Network & System Configuration dialog box

A system administrator can configure the network and system from the **Network & System Configuration** dialog box.

To display the **Network & System Configuration** dialog box, click **Network & System Configuration** in the **Settings** area of the *host-name* window.

System Setup Menu page

You can specify the interface information for a node, network information, and information about external servers to be linked to.

The **System Setup Menu** page first appears after the **Network & System Configuration** dialog box is displayed.

Table C-91 Items displayed on the System Setup Menu page

Item	Description
Setting Type drop-down list	Specify the type of information to be specified or changed. network: Specify settings related to the network. system: Specify settings related to the system.
Display button	Displays the information.

Table C-92 Operations that can be performed when "network" is selected on the System Setup Menu page

Buttons	Description	See
Data Port Setup	Set the negotiation mode for the port.	List of Data Ports page on page C-105
Trunking Setup	Specify trunking for the port.	List of Trunking Configurations page on page C-111
Interface Management	Set interface information.	List of Interfaces page on page C-114
DNS, NIS, LDAP Setup	Set DNS, NIS, and LDAP server information.	DNS, NIS, LDAP Setup page on page C-117
Routing Setup	Set routing information.	List of Routings page on page C-119
Time Setup	Set NTP server information and the time zone.	Time Setup page on page C-122

Table C-93 Operations that can be performed when "system" is selected on the System Setup Menu page

Buttons	Description	See
Syslog Setup	View and set the system log output destination and transfer destination.	Syslog Setup page on page C-123
Log File Capacity Setup	Set the maximum number of log files that can be saved, and the file capacity.	Log File Capacity Setup page on page C-125
Core File Auto. Deletion Setup	Set the storage period for a core file and the time to automatically delete the core file.	Core File Auto. Deletion Setup page on page C-126
Edit System File	Edit the system file.	Edit System File page on page C-126
Performance Tuning	Tune the system performance. However, there is no need to change the settings during normal operation.	Performance Tuning page on page C-133
SNMP Setup	Set the SNMP manager permitted for access and the MIB objects that can be obtained by the SNMP manager.	List of SNMPs page on page C-134

List of Data Ports page

You can check the communication status for a port.

To display the **List of Data Ports** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Data Port Setup** button.

Table C-94 Items displayed on the List of Data Ports page

Item		Description
Data port		The name of the port (either <code>mng0</code> , <code>ethn</code> , or <code>xgben</code>).
Media type		The media type of the port. Copper Metal cables are supported. Fiber Optical cables are supported.
Negotiation mode		The negotiation mode used by the port. Auto Displayed if auto negotiation is used. 10GBase Full Duplex Displayed if 10GBase full duplex communication is used. The negotiation mode is fixed. 1000Base Full Duplex(Auto Negotiation) Displayed if 1000Base full duplex communication is used. Auto negotiation is also used. 100Base Full Duplex Displayed if 100Base full duplex communication is used. The negotiation mode is fixed. 100Base Full Duplex(Auto Negotiation)# Displayed if 100Base full duplex communication is used. Auto negotiation is also used. 100Base Half Duplex Displayed if 100Base half duplex communication is used. The negotiation mode is fixed. 100Base Half Duplex(Auto Negotiation)# Displayed if 100Base half duplex communication is used. Auto negotiation is also used.
Connected status	Link status	The link status. Up The link is operating normally. Down The link is disconnected. Check the negotiation mode of the switch connected to the port, and then set the negotiation mode again. Error

Item	Description
	<p>The link cannot be recognized. An error might have occurred in the HDI system. Download all log files, and contact maintenance personnel.</p>
<p>Speed</p>	<p>The current transfer rate.</p> <p>10GBase Communication is being performed at 10 Gbps.</p> <p>1000Base Communication is being performed at 1 Gbps.</p> <p>100Base Communication is being performed at 100 Mbps.</p> <p>10Base Communication is being performed at 10 Mbps. Note that 10BASE is not a recommended transfer rate. Review the settings of the switch connected to the port to make sure the transfer rate is at least 100BASE.</p> <p>- Communication is not being performed (Link status is Down).</p>
<p>Duplex</p>	<p>The current communication method.</p> <p>Full Full duplex communication is used. This is also displayed when the negotiation mode of the connected switch is auto negotiation and Negotiation mode of the HDI port is <i>Auto</i>.</p> <p>Half Half duplex communication is used. This is also displayed when the negotiation mode of the connected switch is fixed mode (non-auto-negotiation 100Base half duplex, 100Base full duplex, or 10GBase full duplex) and Negotiation mode of the HDI port is <i>Auto</i>.</p> <p>- Communication is not being performed (Link status is Down).</p>
<p>Negotiation Mode Setup button</p>	<p>Changes the negotiation mode of a port. Select the check box for the port whose negotiation mode you want to change, and then click the button. The Negotiation Mode Setup page opens (Negotiation Mode Setup page on page C-107).</p>
<p>#: If the negotiation mode is set to 100Base Full Duplex or 100Base Half Duplex in system versions earlier than 3.2.3, then after an upgrade installation, the negotiation mode is displayed as 100Base Full Duplex(Auto Negotiation) or 100Base Half Duplex(Auto Negotiation).</p>	

Negotiation Mode Setup page

You can change the negotiation mode for a port.



Note: Before you use this page, see [Before changing the negotiation mode for the port: on page C-108](#).

To display the **Negotiation Mode Setup** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Data Port Setup** button. Then, on the **List of Data Ports** page, select the check box for the port for which you want to change the negotiation mode, and then click the **Negotiation Mode Setup** button.

Table C-95 Items displayed on the Negotiation Mode Setup page

Item	Description
ethn	<p>Select a negotiation mode for each <code>ethn</code> from the drop-down list.</p> <p>Auto Select this to use auto negotiation mode for communication.</p> <p>1000Base Full Duplex(Auto Negotiation) Select this to use 1000Base full duplex communication. Auto negotiation is also used.</p> <p>100Base Full Duplex Select this to use 100Base full duplex communication. The negotiation mode is fixed.</p> <p>100Base Half Duplex Select this to use 100Base half duplex communication. The negotiation mode is fixed.</p> <p>100Base Full Duplex(Auto Negotiation) Select this to use 100Base full duplex communication. Auto negotiation is also used.</p> <p>100Base Half Duplex(Auto Negotiation) Select this to use 100Base half duplex communication. Auto negotiation is also used.</p>
mng0	<p>Select a negotiation mode for <code>mng0</code> from the drop-down list. Only Auto is selectable for 10GbE ports.</p> <p>Auto Select this to use auto negotiation mode for communication.</p> <p>1000Base Full Duplex(Auto Negotiation) Select this to use 1000Base full duplex communication. Auto negotiation is also used.</p> <p>100Base Full Duplex Select this to use 100Base full duplex communication. The negotiation mode is fixed.</p> <p>100Base Half Duplex Select this to use 100Base half duplex communication. The negotiation mode is fixed.</p> <p>100Base Full Duplex(Auto Negotiation)</p>

Item	Description
	<p>Select this to use 100Base full duplex communication. Auto negotiation is also used.</p> <p>100Base Half Duplex(Auto Negotiation)</p> <p>Select this to use 100Base half duplex communication. Auto negotiation is also used.</p>
xgben	<p>Select a negotiation mode for each <code>xgben</code> from the drop-down list. When the model of the node is D51B-2U, only Auto is selectable.</p> <p>Auto</p> <p>Select this to use auto negotiation mode for communication. When the model of the node is not D51B-2U, this mode can be selected only when the port supports metal cables.</p> <p>10GBase Full Duplex</p> <p>Select this to use 10GBase full duplex communication. The negotiation mode is fixed. When the model of the node is not D51B-2U, this mode can be selected only when the port supports optical cables.</p> <p>After setting the negotiation mode, confirm that 10GBase is displayed for Speed on the List of Data Ports page. If 10GBase is not displayed, correct the network configuration, such as the settings of the connected switch or LAN cables.</p>

Before changing the negotiation mode for the port:

If you set a negotiation mode that differs from the one set for the connected switch, a linkage error might occur, preventing communication with the port. If communication cannot be established, check whether the negotiation modes for the port and the connected switch are the same. If the negotiation modes are the same, then the problem might be due to a hardware error. If necessary, contact maintenance personnel.

The following table describes the network communication status when the connected switch or HDI is using auto negotiation, and the negotiation modes for a port and the connected switch are different. In addition, [How to check and match the negotiation mode settings for the connected switch and the HDI port on page C-110](#) describes how to check and match the negotiation mode settings for the connected switch and the HDI port.

Table C-96 Network communication status when auto negotiation is being used, and the negotiation modes for a port and the connected switch are different

Negotiation mode for the port	Negotiation mode for the connected switch	Value displayed in Connected status on the List of Data Ports page
Auto negotiation mode (when Auto is set)	Auto negotiation mode	The communication status is chosen, in the following order, depending on the negotiation modes of the

Negotiation mode for the port	Negotiation mode for the connected switch	Value displayed in Connected status on the List of Data Ports page
		port and the connected switch:#1 1. 10GBase full duplex 2. 1000Base full duplex 3. 1000Base half duplex 4. 100Base full duplex 5. 100Base half duplex 6. 10Base full duplex 7. 10Base half duplex Note that, for 10GbE ports, even if auto negotiation mode is enabled for both the port and the connected switch, the following communication cannot be used: 1000Base half duplex communication, 10Base full duplex communication, and 10Base half duplex communication. Note that 10Base is not a recommended communication speed. Correct the setting of the connected switch so that the communication speed is 100Base or greater.
	100Base half duplex	100Base half duplex
	100Base full duplex	100Base half duplex#2
100Base half duplex (when 100Base Half Duplex is set)	Auto negotiation mode	100Base half duplex
100Base full duplex (when 100Base Full Duplex is set)	Auto negotiation mode	100Base full duplex#2
Auto negotiation mode: • 1000Base full duplex (when 1000Base Full Duplex(Auto Negotiation) is set)	Auto negotiation mode	1000Base full duplex
Auto negotiation mode: • 100Base half duplex (when 100Base Half Duplex(Auto Negotiation) is set)	Auto negotiation mode	100Base half duplex
	100Base half duplex	100Base half duplex
	100Base full duplex	100Base half duplex#2

Negotiation mode for the port	Negotiation mode for the connected switch	Value displayed in Connected status on the List of Data Ports page
Auto negotiation mode: • 100Base full duplex (when 100Base Full Duplex(Auto Negotiation) is set)	Auto negotiation mode	100Base full duplex
	100Base half duplex	Communication impossible ^{#2}
	100Base full duplex	Communication impossible ^{#2}
<p>#1: Depending on the switch type, the actual communication speed might be less than expected or communication might become impossible even if auto negotiation mode is set for both the port and switch. In this case, configure the fixed negotiation modes so that the settings on both the port and switch are the same.</p> <p>#2: When one of the connected devices uses auto negotiation mode and the other uses the fixed mode, the device in auto negotiation mode will use the half duplex method. If the other device is using the full duplex method, then communication between the devices might be impossible because the negotiation modes do not match. Even if communication is possible, the throughput and response might degrade.</p>		

How to check and match the negotiation mode settings for the connected switch and the HDI port

The following describes how to check and match the negotiation mode settings for the connected switch and the HDI port.

1. Display the **List of Data Ports** page.
2. Make sure that **Negotiation mode** is **Auto**.
The default mode for the HDI port is **Auto**. If the current mode is not **Auto**, change it to **Auto**.



Note: If **Negotiation mode** of the HDI port is **Auto**, you can identify the negotiation mode of the connected switch in step 4.

3. In **Connected status**, make sure that **Speed** is 100Base or better.
If it is **10Base** or a hyphen (-), a problem may have occurred with a LAN cable, a port, or the connected switch. Resolve the problem.
4. In **Connected status**, review the information in **Duplex** and then take the necessary actions.

If **Duplex** is **Half**:

You can assume that the negotiation mode setting of the connected switch is fixed mode (non-auto-negotiation 100Base half duplex, 100Base full duplex, or 10GBase full duplex).

Change the negotiation mode of the HDI port so that it matches the negotiation mode of the connected switch.

If **Duplex** is **Full**:

You can assume that the negotiation mode setting of the connected switch is auto negotiation.

If you already changed **Negotiation mode** of the HDI port to **Auto** in step 2, you do not need to cancel the change.

List of Trunking Configurations page

You can check the trunking settings.



Note:

- When an interface has been created for a port on which trunking will be set up, edited, or deleted, make sure that the resource group is running normally or was stopped without any problems.
- When you edit the trunking settings, you will temporarily be unable to communicate with or use any services via the interface of the target port.
- If you enable cascaded trunking for a port, always set up a tagged VLAN for that port in order to stabilize communication between the client and the HDI system.
- If trunking settings are configured during operation, the system deletes the interface information (including VLAN settings) set for the port to be trunked and the routing information set for the interface.
- If trunking is released, the system automatically deletes the interface information (including VLAN settings) and routing information set for the port for which trunking is to be released.
- If you have changed the trunking settings, review the interface information, routing information, and VLAN settings.
- You cannot trunk ports that have different negotiation modes or different communication speeds or methods. Check the **List of Data Ports** page in the **Network & System Configuration** dialog box, and trunk only ports that have identical **Negotiation mode**, **Speed**, and **Duplex** settings.

To display the **List of Trunking Configurations** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Trunking Setup** button.

Table C-97 Items displayed on the List of Trunking Configurations page

Item	Description
Trunking configuration	A trunking configuration
Port	<p>A port name.</p> <p><i>agrnumber</i></p> <p>The port is a link aggregation port.</p> <p><i>rdnnumber</i></p> <p>The port is a link alternation port or cascaded trunking port.</p> <p><i>ethnumber</i> or <i>xgbenumber</i></p>

Item	Description				
	The name of a port. When trunking is used, the names of the ports making up trunking are displayed.				
Trunking type	<p>The type of trunking being used.</p> <p>Link Aggregation The port is a link aggregation port.</p> <p>Link Alternation The port is a link alternation port.</p> <p>- Trunking is not set for the port. This is also displayed for the ports making up trunking.</p>				
Link status	<p>The link status of each port.</p> <p>Up The link is operating normally.</p> <p>Down The link is disconnected.</p> <p>Note that, immediately after the trunking settings are changed, Down might be displayed for a port making up trunking even if Up is displayed for the trunking port. Click Refresh in the upper-right corner after waiting a while to update the displayed information.</p>				
MII(ms)	The monitoring interval for the Media Independent Interface link status set for the link aggregation port or the link alternation port.				
LACP	<table border="1"> <tr> <td data-bbox="488 1031 672 1266">Rate</td> <td data-bbox="672 1031 1399 1266"> <p>The LACP interval (interval for checking the status of aggregated ports) set for the link aggregation port.</p> <p>Slow Displayed if the LACP interval is set to 30 seconds.</p> <p>Fast Displayed if the LACP interval is set to 1 second.</p> </td> </tr> <tr> <td data-bbox="488 1266 672 1755">Aggregate</td> <td data-bbox="672 1266 1399 1755"> <p>Displays whether each port is currently aggregated.</p> <p>If Aggregated is displayed for all ports making up the link aggregation port, all the ports have been aggregated.</p> <p>Aggregated Indicates that the port is currently aggregated.</p> <p>Not aggregated Indicates that the port is unable to participate in the aggregation.</p> <p>Note that Not aggregated might be displayed for a port that is normally a participant in the aggregation (for example, the information is obtained immediately after the trunking settings have been changed). Click Refresh in the upper-right corner of the dialog box after a while to update the displayed information.</p> </td> </tr> </table>	Rate	<p>The LACP interval (interval for checking the status of aggregated ports) set for the link aggregation port.</p> <p>Slow Displayed if the LACP interval is set to 30 seconds.</p> <p>Fast Displayed if the LACP interval is set to 1 second.</p>	Aggregate	<p>Displays whether each port is currently aggregated.</p> <p>If Aggregated is displayed for all ports making up the link aggregation port, all the ports have been aggregated.</p> <p>Aggregated Indicates that the port is currently aggregated.</p> <p>Not aggregated Indicates that the port is unable to participate in the aggregation.</p> <p>Note that Not aggregated might be displayed for a port that is normally a participant in the aggregation (for example, the information is obtained immediately after the trunking settings have been changed). Click Refresh in the upper-right corner of the dialog box after a while to update the displayed information.</p>
Rate	<p>The LACP interval (interval for checking the status of aggregated ports) set for the link aggregation port.</p> <p>Slow Displayed if the LACP interval is set to 30 seconds.</p> <p>Fast Displayed if the LACP interval is set to 1 second.</p>				
Aggregate	<p>Displays whether each port is currently aggregated.</p> <p>If Aggregated is displayed for all ports making up the link aggregation port, all the ports have been aggregated.</p> <p>Aggregated Indicates that the port is currently aggregated.</p> <p>Not aggregated Indicates that the port is unable to participate in the aggregation.</p> <p>Note that Not aggregated might be displayed for a port that is normally a participant in the aggregation (for example, the information is obtained immediately after the trunking settings have been changed). Click Refresh in the upper-right corner of the dialog box after a while to update the displayed information.</p>				
Active port	<table border="1"> <tr> <td data-bbox="488 1755 672 1837">Status</td> <td data-bbox="672 1755 1399 1837">The status of the ports for which link alternation is set.</td> </tr> </table> <p>Active</p>	Status	The status of the ports for which link alternation is set.		
Status	The status of the ports for which link alternation is set.				

Item		Description
		Indicates that the port is operating. Standby Indicates that the port is standing by.
	Default	Default is displayed for the link alternation port set to be active port during normal operation.
Create Link Aggregation button		Click to set link aggregation. Select the ports you want to specify for link aggregation, and then click this button. The Link Aggregation Setup page opens (Link Aggregation Setup page on page C-113).
Create Link Alternation button		Click to set link alternation. Select the two ports you want to specify for link alternation, and then click this button. The Link Alternation Setup page opens (Link Alternation Setup page on page C-114).
Edit Trunking button		Click to change the trunking settings. Select the ports whose settings you want to change, and then click this button. The Link Aggregation Setup page or the Link Alternation Setup page opens (Link Aggregation Setup page on page C-113 or Link Alternation Setup page on page C-114). To change a link aggregation port, click the Release Trunking button to cancel the link aggregation settings, and then click the Edit Trunking button to set up link aggregation again.
Release Trunking button		Click to release trunking. Select the trunking you want to release, and then click this button.
Change Active Port Status button		Click to change the link. Select the port whose link status you want to change, and then click this button.

Link Aggregation Setup page

You can set up link aggregation.

To display the **Link Aggregation Setup** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Trunking Setup** button. Then, on the **List of Trunking Configurations** page, select the ports for which you want to set up link aggregation, and then click the **Create Link Aggregation** button.

Table C-98 Items displayed on the Link Aggregation Setup page

Item	Description
LACP rate drop-down list	Use this drop-down list to select the interval for checking the status of the ports making up a link aggregation port. Slow: Checks the status every 30 seconds. Fast: Checks the status every second.

Item	Description
MII	Specify the interval at which the status of the Media Independent Interface link is checked. You can specify a value from 1 to 100 in 10-ms units.

Link Alternation Setup page

You can set up link alternation.

To display the **Link Alternation Setup** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Trunking Setup** button. Then, on the **List of Trunking Configurations** page, select the two ports for which you want to set up link alternation, and then click the **Create Link Alternation** button.

Table C-99 Items displayed on the Link Alternation Setup page

Item	Description
Default active port drop-down list	Use this drop-down list to select the port that is to be used during normal operation. Select a port whose status is normal. You can check the link status in Link status on the List of Trunking Configurations page.
MII	Specify the interval at which the status of the Media Independent Interface link is checked. You can specify a value from 1 to 100 in 10-ms units.

List of Interfaces page

You can check the interface information.

To display the **List of Interfaces** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Interface Management** button.

Table C-100 Items displayed on the List of Interfaces page

Item	Description
Protocol version drop-down list	From the drop-down list, select the protocol version for which you want to check the interface information, and then click the Display button.
Port drop-down list	From the drop-down list, select the port whose interface information you want to check, and then click the Display button.
Interface	Port
	VLAN ID
	The port name.
	The VLAN ID. A hyphen (-) is displayed if a VLAN is not used.
DHCP	When IPv4 is used, displays whether DHCP was used in setting the port interface information.

Item	Description
IP address	The IP address
Netmask	The netmask is displayed if IPv4 is used.
Prefix length	The prefix length is displayed if IPv6 is used.
MTU	The MTU value.
Edit button	Click to edit the interface information. Use a radio button to select the interface you want to edit, and then click this button. The Edit Interface page opens (Edit Interface page on page C-115).
Delete button	Click to delete the interface information. Use a radio button to select the interface you want to delete, and then click this button.
Add button	Click to set interface information. The Add Interface page opens (Add Interface page on page C-116).

Edit Interface page

You can change the interface information.



Note: After changing the interface information, perform the following if necessary:

- If you have changed the MTU value, make sure that communication can be performed between the client and the node at the highest MTU value. To do this, use the `ping` command from the client after making the change. If the MTU value is set correctly, but the client cannot communicate with the node, a peripheral device or client might be the cause of the problem. Check the peripheral device and client settings.
- If you have changed the **IP address**, **Netmask**, or **Prefix length** value for `mng0`, after clicking the **OK** button, click the **Close** button in the dialog box that appears. To continue operation, wait a while, and then log on to the GUI.
- If the GUI does not respond, click the **x** button in the title bar to close the window.

To display the **Edit Interface** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Interface Management** button. Then, on the **List of Interfaces** page, select the radio button for the interface for which you want to edit the information, and then click the **Edit** button.

Table C-101 Items displayed on the Edit Interface page

Item	Description
Port	The port name.
VLAN ID	The VLAN ID. A hyphen (-) is displayed if a VLAN is not used.

Item	Description
	If the <code>mng0</code> information is edited, this item is not displayed.
IP address#	Specify the IP address.
Netmask	Specify the netmask if IPv4 is used.
Prefix length	Specify the prefix length if IPv6 is used.
MTU	<p>Specify the MTU value of an interface. Changing the MTU value of the interface allows you to use the Jumbo Frame packet.</p> <p>A value ranging from 1280 to 9216 can be specified for a GbE port, and a value ranging from 1280 to 16110 can be specified for a 10 GbE port. However, depending on the hardware type and configuration, the maximum specifiable value for a GbE port might be 9000, and the maximum specifiable value for a 10 GbE port might be 9600.</p> <p>The value specified here is applied to both the IPv4 and IPv6 environments.</p> <p>Note that the MTU value for <code>mng0</code> cannot be changed.</p>
<p>#: The IP addresses of the networks listed below cannot be specified. If specifying one of these is unavoidable, contact the Technical Support Center.</p> <ul style="list-style-type: none"> IPv4: 127.0.0.0 to 127.255.255.255 IPv6: "::ffff:IPv4-address", "::IPv4-address", ":::1/128", ":::/0", ":::/128", "fe80::/10", and "ff00::/8" Network whose IP address is set in <code>pm0</code> 	

Add Interface page

You can add interface information.



Note: If you have changed the MTU value, make sure that communication can be performed between the client and the node at the highest MTU value. To do this, use the `ping` command from the client after making the change. If the MTU value is set correctly, but the client cannot communicate with the node, a peripheral device or client might be the cause of the problem. Check the peripheral device and client settings.

To display the **Add Interface** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Interface Management** button. Then, on the **List of Interfaces** page, click the **Add** button.

Table C-102 Items displayed on the Add Interface page

Item	Description
Port drop-down list	Select the port you want to add. The name of the port using a VLAN is followed by (Use VLAN). If you select a port name followed by (Use VLAN), select Use for Tagged VLAN .
Tagged VLAN	Select whether to use a tagged VLAN. Use: Use a tagged VLAN. Enter any VLAN ID for VLAN ID .

Item	Description
	Do not use: Do not use a tagged VLAN.
IP address#	Specify the IP address.
Netmask	Specify the netmask if IPv4 is used.
Prefix length	Specify the prefix length if IPv6 is used.
MTU	<p>Specify the MTU value of an interface. Changing the MTU value of the interface allows you to use the Jumbo Frame packet.</p> <p>A value ranging from 1280 to 9216 can be specified for a GbE port, and a value ranging from 1280 to 16110 can be specified for a 10 GbE port. However, depending on the hardware type and configuration, the maximum specifiable value for a GbE port might be 9000, and the maximum specifiable value for a 10 GbE port might be 9600.</p> <p>The value specified here is applied to both the IPv4 and IPv6 environments.</p>
<p>#: The IP addresses of the networks listed below cannot be specified. If specifying one of these is unavoidable, contact the Technical Support Center.</p> <ul style="list-style-type: none"> • IPv4: 127.0.0.0 to 127.255.255.255 • IPv6: "::ffff:IPv4-address", "::IPv4-address", ":::1/128", ":::/0", ":::/128", "fe80::/10", and "ff00::/8" • Network whose IP address is set in pm0 	

DNS, NIS, LDAP Setup page

You can change the information about a DNS server, NIS server, and user authentication LDAP server.



Note: A maximum of two DNS servers, two NIS servers, and two LDAP servers can be specified. When two servers of the same type are specified, if a failure occurs on the server that is running, operation continues by automatically switching to the other server.

After changing the information, use the **Check for Errors** dialog box to display the **List of RAS Information** page (for `Server check`), and then confirm that each server has been set up correctly.

Then, restart the node, FTP or SFTP service.

Restart the node when:

- **NIS setup** information is set, changed, or deleted.
- **DNS setup** information is set or changed.
- New **LDAP setup (for user authentication)** information is set, or all information that has been set is released.

Restart the FTP or SFTP services when:

LDAP setup (for user authentication) information is changed.

To display the **DNS, NIS, LDAP Setup** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **DNS, NIS, LDAP Setup** button.

Table C-103 Items displayed on the DNS, NIS, LDAP Setup page

Item	Description	
DNS setup	When you use the DNS server, specify information about the DNS server. When you do not use the DNS server, you can omit specification of this item.	
	Default domain name	Specify the name of the domain to which the nodes belong. Enter a maximum of 255 characters. You can omit this setting if domain names are not being used. You can enter alphanumeric characters, a hyphen (-), and a period (.). Assuming that the number of domains to be specified is n , and the total number of characters for all domain names is m , the following expression must be satisfied: $m + (n - 1) \leq 255$
	Search domain names	If there are domains that you want to set as name resolution search targets other than the domain specified in Default domain name , specify the names of the target domains. You can specify a maximum of five domain names. You can enter alphanumeric characters, a hyphen (-), and a period (.). The search is performed in the order of the domains in the text boxes. Assuming that the number of domains to be specified is n , and the total number of characters for all domain names is m , the following expression must be satisfied: $m + (n - 1) \leq 255$
	Primary DNS server	Specify the IP address of the DNS server to be used for normal operation.
	Secondary DNS server	Specify the IP address of the DNS server to be used if the primary DNS server fails.
NIS setup	When you want to use the NIS server, specify information about the NIS server. When you do not want to use the NIS server, you can omit specification of this item. If you specify an invalid value, it might not be possible to set the network information.	
	NIS domain	In the text box, specify the name of the domain that the NIS server belongs to. In addition, use a radio button to select the NIS server you want to use. NIS server specification Select this when you want to use a specific NIS server. In NIS server(s) , specify the IP address or server name of the NIS server you want to use (the IP address is recommended). If you specify two NIS servers, the NIS server that is specified first will be used during

Item	Description	
		<p>normal operation. If this NIS server fails, the other NIS server will be used.</p> <p>Broadcast specification</p> <p>Select this when you want to use broadcasting and it does not matter which NIS server on the network is used.</p>
<p>LDAP setup (for user authentication)</p>	<p>When you want to use the LDAP server to authenticate users, specify information about the LDAP server. When you do not want to use the LDAP server, you can omit specification of this item.</p> <p>Ask the LDAP server administrator for the information necessary to specify the values.</p>	
	<p>LDAP server(s)</p>	<p>In the text box, specify the IP address or server name of the LDAP server you want to use (the IP address is recommended). If you specify two LDAP servers, the LDAP server that is specified first will be used during normal operation. If this LDAP server fails, the other LDAP server will be used.</p> <p>In addition, specify the port number of the LDAP server in the Port text box. When this specification is omitted, 389 is set.</p>
	<p>LDAP server root DN</p>	<p>Specify the root identification name of the LDAP server in DN format, as in the following example:</p> <p><code>dc=hitachi,dc=co,dc=jp</code></p>
	<p>LDAP administrator DN</p>	<p>Specify the identification name of the LDAP server administrator in DN format, as in the following example:</p> <p><code>cn=Administrator,dc=hitachi,dc=co,dc=jp</code></p> <p>Make sure that you specify this item when an end user logs on to the HDI system via the GUI and the security settings for the LDAP server that will be used do not allow an anonymous user to obtain a password.</p>
	<p>LDAP administrator password</p>	<p>Specify the password of the LDAP server administrator.</p> <p>Make sure that you specify this item when an end user logs on to the HDI system via the GUI and the security settings for the LDAP server that will be used do not allow an anonymous user to obtain a password.</p>

List of Routings page

A system administrator can check the routing information in the List of Routings page.

To display the **List of Routings** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Routing Setup** button.

Table C-104 Items displayed on the List of Routings page

Item		Description
Protocol version drop-down list		From the drop-down list, select the protocol version whose routing information you want to check, and then click the Display button.
Port drop-down list		From the drop-down list, select the port whose routing information you want to check, and then click the Display button.
Interface	Port	The port name
	VLAN ID	The VLAN ID is displayed if a VLAN is used. A hyphen (-) is displayed if a VLAN is not used.
DHCP		When IPv4 is used, displays whether DHCP was used in setting the port routing information.
Target		The routing destination. The IP address, host name, or network name of the target is displayed. If the default route has been specified, <code>default</code> is displayed.
Netmask		If IPv4 is used, the netmask is displayed for a network. For a host, a hyphen (-) is displayed. If the default route is set for the routing destination, <code>0.0.0.0</code> is displayed.
Prefix length		If IPv6 is used, the prefix length is displayed for a network. For a host, a hyphen (-) is displayed. If the default route is set for the routing destination, <code>0</code> is displayed.
Gateway		The IP address or host name of the gateway through which network data is routed
Method of specifying route		Displays whether a route has been set or denied for the routing target. Allow A route has been set for the routing target. Reject A route has been denied for the routing target.
MSS		If IPv4 is used, the maximum segment size for the TCP connection on the route is displayed.
Delete button		Click to delete the routing information. Use a radio button to select the routing information you want to delete, and then click this button.
Add button		Click to add routing information. The Add Routing page opens (Add Routing page on page C-120).

Add Routing page

A system administrator can add a routing information.



Note:

- Make sure that there are no more than 512 items of routing information.

- You cannot specify routing targets that the system administrator set in the routing information.
On the **List of Routings** page, you can check routing targets that the system administrator set in the routing information.
- You cannot specify routing targets that the system set automatically in the routing information.
You can use the `routelist -l` command to check routing targets that the system set automatically.
- The HDI system might be unable to respond to an ICMP redirect request from a gateway (request to change the route to another gateway). Therefore, the network must be designed so that no ICMP redirect occurs. Note that multiple gateways that connect to one or more external network segments can exist in a network segment connected to an HDI port. In such an environment, set the routing information so that an appropriate gateway is used for each of the external network addresses that the HDI system must communicate with.

To display the **Add Routing** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Routing Setup** button. Then, from the **Protocol version** drop-down list on the **List of Routings** page, select the protocol version for which you want to add information, and then click the **Add** button.

Table C-105 Items displayed on the Add Routing page

Item	Description
Interface	Select the target interface information. Port Select the target port from the drop-down list. VLAN ID If you select a port using a VLAN for Port , select the target VLAN ID from the drop-down list. This item is blank if a VLAN is not used.
How to specify target ^{#1}	Select the method to be used to specify the routing destination. Only one default route can be specified. Network Specify the destination by using the network address. Host Specify the target by using the host name or IP address. Default route Specify the default route.
Target ^{#2}	Specify the routing destination in the format you selected in How to specify target . If you select Default route in How to specify target , <code>default</code> is displayed.
Netmask ^{#1}	If IPv4 is used and Network is selected in How to specify target , specify the netmask.

Item	Description
	If either Host or Default route is selected, you do not need to specify the netmask. If you specify the netmask, the specification is ignored.
Prefix length ^{#1}	If IPv6 is used and Prefix length is selected in How to specify target , specify the prefix length. If either Host or Default route is selected, you do not need to specify the prefix length. If you specify the prefix length, the specification is ignored.
Gateway ^{#2}	Enter the IP address or host name of the gateway through which network data is to be routed.
Method of specifying route	Use a radio button to determine whether a route has been set or denied for the routing setting target. Allow Set a route. Reject Deny routing.
MSS	If IPv4 is used, specify in bytes the maximum segment size for the TCP connection on the route. Enter a value in the range from 64 to 65536.
<p>#1:</p> <ul style="list-style-type: none"> The route added by selecting Network in How to specify target and specifying 0.0.0.0 for Netmask or 0 for Prefix length is treated as the default route. The routing added by selecting Network in How to specify target and specifying 255.255.255.255 for Netmask or 128 for Prefix length works the same as when the host is directly specified for the routing destination. <p>#2:</p> <p>The IP addresses of the networks listed below cannot be specified as the routing destination. If specifying one of these is unavoidable, contact the Technical Support Center.</p> <ul style="list-style-type: none"> IPv4: 127.0.0.0 to 127.255.255.255 IPv6: "::ffff:IPv4-address", "::IPv4-address", ":::1/128", ":::/0", ":::/128", "fe80::/10", and "ff00::/8" Network whose IP address is set in pm0 	

Time Setup page

You can specify time-related information.



Note:

- HDI systems use an NTP server to synchronize the times of client machines that use the file systems and the node times.
- When the **System Setup Menu** page opens in the dialog box, restart the node.
If an NTP server is specified, after the node has been restarted, view the **List of RAS Information** page (for List of messages) in the **Check for**

Errors dialog box to make sure that the system message KAQM05154-I has been output.

To display the **Time Setup** page, select **network** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Time Setup** button.

Table C-106 Items displayed in the NTP setup area and the Time zone setup area on the Time Setup page

Item	Description
NTP server(s)	Specify one or two IP addresses or host names when you use an NTP server. We recommend that you specify IP addresses or host names for two different NTP servers as a countermeasure against a failure. Do not specify two host names for the same NTP server. When two NTP servers are specified, if a failure occurs on the server that is running, operation continues by automatically switching to the other server.
Time zone	Select the time zone. The time zone is displayed in directory structure. Select a time zone from the list box, and then click the Select button. If lower levels are included in the selected time zone, it is expanded to the immediately lower time zones when you click the Select button. To go back to the upper levels, select .. , and then click the Select button. For example, to set the time zone to Japan, select Asia , and then Tokyo , or select Japan . To set the time zone to Los Angeles, select America , and then Los_Angeles . We recommend that you set the time zone by selecting a city name. If the time zone is set to the GMT format, the time zone offset is displayed with + for zones west of the Greenwich meridian and - for zones east of it.

Syslog Setup page

You can view the contents of a system log configuration file.

To display the **Syslog Setup** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Syslog Setup** button.

Table C-107 Items displayed on the Syslog Setup page

Item	Description
Item name	The facilities and priorities set in selector fields of the system log configuration file.
Output destination	The host names of the transfer destinations for message logs about facilities and priorities, and the output destinations of logs used in an HDI system.

Item	Description
Edit button	Click to change the transfer destination of system logs. Use a radio button to select the item you want to change, and then click this button. The Edit Syslog Setup page opens (Edit Syslog Setup page on page C-124).
Delete button	Click to delete the system log transfer destination. Use a radio button to select the item you want to delete, and then click this button.
Add button	Click to add transfer destination for system logs. The Add Syslog Setup page opens (Add Syslog Setup page on page C-124).

Edit Syslog Setup page

You can change the system log transfer destination.



Note: A value whose format is not *@host-name* in **Output destination** cannot be changed.

To display the **Edit Syslog Setup** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Syslog Setup** button. Then, on the **Syslog Setup** page, select the radio button for the item to be changed, and then click the **Edit** button.

Table C-108 Items displayed on the Edit Syslog Setup page

Item	Description
Item name	Specify a facility and its priority to be set in a selector field of the system log configuration file.
Output destination	Specify a transfer destination for message logs about the facility and its priority. Specify the destination host name in the format <i>@host-name</i> .

Add Syslog Setup page

You can add a system log transfer destination.

To display the **Add Syslog Setup** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Syslog Setup** button. Then, on the **Syslog Setup** page, click the **Add** button.

Table C-109 Items displayed on the Add Syslog Setup page

Item	Description
Item name	Specify a facility and its priority to be set in a selector field of the system log configuration file.

Item	Description
Output destination	Specify a transfer destination for message logs about the facility and its priority. Specify the destination host name in the format <i>@host-name</i> .
Add button	Adds a system log transfer destination. Enter the necessary information, and then click this button.

Log File Capacity Setup page

You can view the number of files saved in a log file and the log file capacity.



Note: Log files that have already been output are not automatically deleted even if you reduce the number of log files to be saved. If necessary, from the **List of RAS Information** page, delete the old log files.

To display the **Log File Capacity Setup** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Log File Capacity Setup** button.

Table C-110 Items displayed on the Log File Capacity Setup page

Item	Description
File type	The log file type as a path
Capacity (MB)	The capacity of the log files
Number of files	The number of files that can be saved in a log file
Explanation	An explanation of the log file
Edit button	Click to change the number of files saved in a log file and the capacity. Use a radio button to select the log file whose settings you want to change, and then click this button. The Edit File Capacity page opens (Edit File Capacity page on page C-125).

Edit File Capacity page

A system administrator can change the maximum number of log files that can be saved, and the file capacity.

To display the **Edit File Capacity** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Log File Capacity Setup** button. Then, on the **Log File Capacity Setup** page, select the radio button for the log file for which you want to change the settings, and then click the **Edit** button.

Table C-111 Items displayed on the Edit File Capacity page

Item	Description
File type	The log file type as a path.

Item	Description
Capacity drop-down list	Select a value from 1 to 6 for the maximum size of the log file (units: MB). If the log file exceeds the maximum size, the file will be switched to the next generation.
Number of files drop-down list	Specify the number of files that can be saved in a log file. The values specified here means all log files except the current log file. If the number of saved log files exceeds the specified number of files, excess files are deleted starting from the oldest file. You can select a value from 1 to 14.

Core File Auto. Deletion Setup page

You can specify a retention period for core files and a time for files to be automatically deleted.



Note: If you specify a retention period for core files and a time when files are deleted automatically, core files whose retention period has expired are deleted automatically at the specified time. When core files are deleted automatically, space becomes available in the area in which log files and core files are saved on the OS disk.

To display the **Core File Auto. Deletion Setup** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Core File Auto. Deletion Setup** button.

Table C-112 Items displayed on the Core File Auto. Deletion Setup page

Item	Description
Period to save	Specify the core file retention period as a number of days. Specify a value from 0 to 99. When the retention period expires, a core file is deleted at the time specified for Automatic deletion time .
Automatic deletion time	Specify in hours and minutes the time at which a core is checked and automatic deletion is performed. Specify a value from 00:00 to 23:55 five-minute interval.
Add button	Click this button to add the time specified in Automatic deletion time to the list box. Times that are not listed in the list box are not set as times for checking and automatically deleting the core file.
Delete button	Click this button to delete a time from the list box. First select the time you want to delete, and then click this button.

Edit System File page

In the **Edit System File** page, the system administrator can directly edit system files of the HDI system.

**Note:**

- Host names can be specified using alphanumeric characters, hyphens (-), and periods (.).
- If you have edited the `/etc/hosts` file or the `/etc/cifs/lmhosts` file, you need to restart the NFS or CIFS service.

To display the **Edit System File** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Edit System File** button.

Table C-113 Items displayed on the Edit System File page

Item	Description						
File type drop-down list	<p>Select the system file you want to edit from the drop-down list. After selecting the system file, click the Display button.</p> <table border="1" data-bbox="545 667 1513 1795"> <tr> <td data-bbox="545 667 753 1157"> /etc/hosts </td> <td data-bbox="753 667 1513 1157"> <p>Associates host names with IP addresses when host information is managed. Do not change or delete the values that were set in the <code>hosts</code> file when operation started.</p> <p>If NFS file locking is used from the public destination host for an NFS share, add the following information:</p> <ul style="list-style-type: none"> • IP address and host name of the resource group to which an NFS share to be mounted belongs • IP address and host name of the NFS client host that uses NFS file locks <p>In addition, if you use a host name for limiting the public destination for CIFS services and CIFS share, in Host access restrictions on the CIFS Service Management (Security) page in the Access Protocol Configuration dialog box, add the host name and the IP address of the CIFS client to allow or prohibit CIFS access.</p> </td> </tr> <tr> <td data-bbox="545 1157 753 1346"> /etc/cifs/lmhosts </td> <td data-bbox="753 1157 1513 1346"> <p>For NT domain authentication or Active Directory authentication, this file associates NT domain controllers' IP addresses with domain names for the NT domains that have trust relationships. Append the following line to this file:</p> <p><i>IP-address NetBIOS-domain-name-for-domain-controller-that-has-trust-relationship</i></p> </td> </tr> <tr> <td data-bbox="545 1346 753 1795"> /etc/snmp/snmpd.conf^{#1} </td> <td data-bbox="753 1346 1513 1795"> <p>SNMP setup file.</p> <p>To enable SNMP trap notification for SNMPv2, append the following to this file:</p> <p>IPv4 environment:</p> <pre>trap2sink SNMP-manager-host-name-or-IP-address [community-name [port-number]]</pre> <p>Example: <code>trap2sink 10.213.76.194 stdDefComm1</code></p> <p>IPv6 environment:</p> <pre>trap2sink udp6:SNMP-manager-host-name-or-IP-address#1:port-number [community-name]</pre> <p>Example: <code>trap2sink udp6:ip6-winhost1:162 stdDefComm1</code></p> </td> </tr> </table>	/etc/hosts	<p>Associates host names with IP addresses when host information is managed. Do not change or delete the values that were set in the <code>hosts</code> file when operation started.</p> <p>If NFS file locking is used from the public destination host for an NFS share, add the following information:</p> <ul style="list-style-type: none"> • IP address and host name of the resource group to which an NFS share to be mounted belongs • IP address and host name of the NFS client host that uses NFS file locks <p>In addition, if you use a host name for limiting the public destination for CIFS services and CIFS share, in Host access restrictions on the CIFS Service Management (Security) page in the Access Protocol Configuration dialog box, add the host name and the IP address of the CIFS client to allow or prohibit CIFS access.</p>	/etc/cifs/lmhosts	<p>For NT domain authentication or Active Directory authentication, this file associates NT domain controllers' IP addresses with domain names for the NT domains that have trust relationships. Append the following line to this file:</p> <p><i>IP-address NetBIOS-domain-name-for-domain-controller-that-has-trust-relationship</i></p>	/etc/snmp/snmpd.conf ^{#1}	<p>SNMP setup file.</p> <p>To enable SNMP trap notification for SNMPv2, append the following to this file:</p> <p>IPv4 environment:</p> <pre>trap2sink SNMP-manager-host-name-or-IP-address [community-name [port-number]]</pre> <p>Example: <code>trap2sink 10.213.76.194 stdDefComm1</code></p> <p>IPv6 environment:</p> <pre>trap2sink udp6:SNMP-manager-host-name-or-IP-address#1:port-number [community-name]</pre> <p>Example: <code>trap2sink udp6:ip6-winhost1:162 stdDefComm1</code></p>
/etc/hosts	<p>Associates host names with IP addresses when host information is managed. Do not change or delete the values that were set in the <code>hosts</code> file when operation started.</p> <p>If NFS file locking is used from the public destination host for an NFS share, add the following information:</p> <ul style="list-style-type: none"> • IP address and host name of the resource group to which an NFS share to be mounted belongs • IP address and host name of the NFS client host that uses NFS file locks <p>In addition, if you use a host name for limiting the public destination for CIFS services and CIFS share, in Host access restrictions on the CIFS Service Management (Security) page in the Access Protocol Configuration dialog box, add the host name and the IP address of the CIFS client to allow or prohibit CIFS access.</p>						
/etc/cifs/lmhosts	<p>For NT domain authentication or Active Directory authentication, this file associates NT domain controllers' IP addresses with domain names for the NT domains that have trust relationships. Append the following line to this file:</p> <p><i>IP-address NetBIOS-domain-name-for-domain-controller-that-has-trust-relationship</i></p>						
/etc/snmp/snmpd.conf ^{#1}	<p>SNMP setup file.</p> <p>To enable SNMP trap notification for SNMPv2, append the following to this file:</p> <p>IPv4 environment:</p> <pre>trap2sink SNMP-manager-host-name-or-IP-address [community-name [port-number]]</pre> <p>Example: <code>trap2sink 10.213.76.194 stdDefComm1</code></p> <p>IPv6 environment:</p> <pre>trap2sink udp6:SNMP-manager-host-name-or-IP-address#1:port-number [community-name]</pre> <p>Example: <code>trap2sink udp6:ip6-winhost1:162 stdDefComm1</code></p>						

Item	Description
	<p>If you want to use a specific IP address as the trap notification source, also add the following setting:</p> <pre>sending_srcaddress SNMP-manager-host-name-or-IP-address#1 notification-source-IP-address#1</pre> <p>Specify a community name using no more than 32 characters.</p> <p>You can specify ASCII alphanumeric characters and the following ASCII symbols:</p> <pre># % + - . / : = @ _</pre> <p>A hash mark (#) cannot be used for the first character of a community name.</p> <p>The default community name is <code>private</code>, and the default port number is <code>162</code>.</p> <p>If you configure trap notification, make sure that the <code>cold start trap</code> is issued after the file is updated. If the trap is not issued, check the contents of the file. If you omit the community name for <code>trap2sink</code>, <code>public</code> is set for the community name of the <code>cold start</code> and <code>nsNotifyShutdown</code> traps that are issued when <code>snmpd</code> is started and stopped.</p> <hr/> <p>To use SNMPv3, add the following entries as SNMP administration user setting information at the end of the file:</p> <pre>rouser user-name [security-level [OID]] createUser user-name [authentication-type authentication-password [encryption-type encryption-password]]</pre> <p>Example:</p> <pre>rouser user1 priv createUser user1 MD5 mypassphrase DES mypassword</pre> <p><code>rwuser</code> can be specified instead of <code>rouser</code>.</p> <p>For details about the items to be specified when SNMPv3 is used, see Table 10-1 Information specified in the snmpd.conf file when SNMPv3 is used on page 10-4.</p> <p>To acquire the operational status of the system via SNMPv3, edit the <code>group</code>, <code>view</code>, and <code>access</code> entries in the Access Control column as in the following procedure. If these entries do not exist, add them.</p> <p>group:</p> <p>In the Access Control column, you write after the line <code># Second</code>, map the security names into group names: is followed:</p> <pre>group group-name security-model user-name</pre> <p>For <code>user-name</code>, specify the user name that was specified in the <code>rouser</code> or <code>rwuser</code> entry. For <code>security-model</code>, specify <code>usm</code>.</p> <p>view:</p> <p>In the Access Control column, you write after the line <code># Third</code>, create a view for us to let the groups have rights to: is followed:</p> <pre>view view-name type OID mask</pre>

Item	Description
	<p>For <i>OID</i> and <i>mask</i>, specify the OID and mask of the MIB object that is acquired by the SNMP manager. For <i>type</i>, to include subtrees of the OID, specify <i>included</i>. To exclude subtrees of the OID, specify <i>excluded</i>. For details about the relevant MIB object, see section MIB objects for responding to SNMP get requests on page F-3.</p> <p>access</p> <p>In the Access Control column, you write after the line # Finally, grant the 2 groups access to the 1 view with different: is followed:</p> <pre>access group-name context security-model security-level prefix READ-view WRITE-view NOTIFY-view</pre> <p>For <i>context</i>, specify "". For <i>security-model</i>, specify <i>any</i> or <i>usm</i>. Because HDI system does not support writing to MIB objects, specify a view for only <i>READ-view</i>, and <i>none</i> for <i>WRITE-view</i> and <i>NOTIFY-view</i>. For <i>security-level</i>, specify the security level (<i>noauth</i>, <i>auth</i>, or <i>priv</i>) that was specified in the <i>rouser</i> or <i>rwuser</i> entry.</p> <p>Note that even if you want to permit MIB object acquisition via SNMPv3 only, you must set the local host (<i>localhost</i>) by editing the <i>com2sec</i> entry in the Access Control column. In this case, edit the <i>snmpd.conf</i> file on the Edit System File page.</p> <p>For an example of specifying the settings in the <i>snmpd.conf</i> file when using SNMPv3, see Example C-1 Example of specifying the settings in the snmpd.conf file when using SNMPv3 on page C-133.</p> <hr/> <p>To enable SNMP trap notification for SNMPv3, append the following to this file:</p> <p>IPv4 environment:</p> <pre>trapsess -v3 -u user-name [option] SNMP-manager-host-name-or-IP-address[:port-number]</pre> <p>Example: <code>trapsess -v3 -u user1 -l authPriv -a MD5 -A mypassphrase -x DES -X mypassword 10.213.76.194</code></p> <p>IPv6 environment:</p> <pre>trapsess -v3 -u user-name [option] udp6:SNMP-manager-host-name-or-IP-address#1[:port-number]</pre> <p>Example: <code>trapsess -v3 -u user1 -l authPriv -a MD5 -A mypassphrase -x DES -X mypassword udp6:[2001:0db8:bd05:01d2:288a:1fc0:0001:10ee]:162</code></p> <p>If you want to use a specific IP address as the trap notification source, also add the following setting:</p> <pre>sending_srcaddress SNMP-manager-host-name-or-IP-address#1 notification-source-IP-address#1</pre> <p>The default port number is 162.</p> <p>Do not specify options that issue SNMPv2 traps usable by <i>net-snmp</i>.</p>

Item	Description
	<p>For details about the items to be specified when SNMPv3 is used, see Table 10-1 Information specified in the snmpd.conf file when SNMPv3 is used on page 10-4.</p> <p>To use SNMPv2 in an IPv6 environment to obtain the system operating status, edit <code>com2sec</code>, <code>com2sec6</code>, <code>group</code>, <code>view</code>, and <code>access</code> in <code>Access Control</code> for the SNMP manager permitted for access and MIB objects that can be obtained.</p> <p>To use SNMPv2 in an IPv4 environment to obtain the system operating status, in the List of SNMPs page, you need to specify the SNMP manager permitted for access and MIB objects that can be obtained. If you need to directly edit the <code>snmpd.conf</code> file, contact the customer support.</p> <p>When you are using SNMPv2 in an IPv6 environment or SNMPv3 to obtain the system operating status, the default settings are specified so that any host in the network can access MIB objects.</p> <p>If you are using SNMPv2 in an IPv6 environment, perform either of the following procedures when you restrict access so that only specified SNMP managers have access to MIB objects:</p> <ul style="list-style-type: none"> • Delete any instances of <code>com2sec6</code> in <code>Access Control</code> for which the <code>source</code> is set to the <code>default</code>. • Add a hash mark (#) to the beginning of the relevant lines. <p>Then, add the server name of the SNMP manager permitted for access. You can specify multiple SNMP managers.</p> <p>If you are using SNMPv3, you cannot restrict which SNMP managers have access to MIB objects.</p> <p>If you do not obtain the system operating status, delete all entries or change them to comments, and then add the local host (<code>localhost</code>).</p> <p>In addition, for <code>view</code>, add the MIB objects that can be obtained by the SNMP manager. For details about the MIB objects to be specified, see section MIB objects for responding to SNMP get requests on page F-3.</p> <p>To set whether to provide quota information depending on the number of registered users and groups for a file system, append the following line to the end of the file. You can specify the maximum value in the range from 0 to 2,147,483,147. If you specify 0, quota information is not provided.</p> <pre>std_quota_max maximum-number std_stquota_max maximum-number</pre> <p>To prevent the acquisition of the MIB objects from being interrupted, you can specify settings so that the SNMP agent does not restart during the mounting of a file system.</p> <p>When specifying settings to prevent the SNMP agent from restarting, append the line below to the file. Note that the restart of the SNMP agent is not suppressed when <code>snmpd.conf</code> is updated, or when a restart operation scheduled daily at 00:01 is executed.</p>

Item	Description
	<pre>reboot_on_resource_event off</pre> <p>To obtain the most recent information about the MIB object in <code>dskEntry</code> when you have specified settings to prevent the SNMP agent from restarting, append the following line to the file:</p> <pre>Fixed-order_path on disk path-of-the-file-system-from-which-information-is-to-be-obtained unused-capacity</pre> <p>In this setting, the MIB object is applied to the file systems that are unmounted, and the index is fixed. At this time, a null string is set to the device name, and "0" is set to the MIB object that indicates the capacity.</p> <p>The following is an example of obtaining the most recent information about <code>fs01</code> and <code>fs02</code> file systems by the MIB object in <code>dskEntry</code> by suppressing a restart:</p> <pre>reboot_on_resource_event off Fixed-order_path on disk /mnt/fs01 10% disk /mnt/fs02 10%</pre> <p>To set the file system whose status is acquired and set the unused capacity level of the file system from which an error is sent, append the following line to the end of the file.</p> <pre>disk file-system-path unused-capacity</pre> <p>With this setting, SNMP traps are not reported. You need to use the <code>fsctl</code> command to specify that SNMP traps are to be reported whenever the usage amount of the file system exceeds a threshold.</p> <p>Example of acquiring the status of the <code>fs01</code> file system and sending an error when the unused capacity goes down to 10%: <code>disk /mnt/fs01 10%</code></p> <p>For information about file systems, to make a restriction so that only information related to a specific object is reported, specify the following for each information item:</p> <p>Specific file system information: <code>fspath file-system-path</code></p> <p>Example of reporting the information of the file systems <code>fs01</code> and <code>fs02</code>:</p> <pre>fspath /mnt/fs01 fspath /mnt/fs02</pre>
<p>/enas/conf/email_alert.conf</p>	<p>The configuration file for email error notifications. Specify values for the entries in the configuration file as follows:</p> <pre>serveraddress=mail-server-fully-qualified-domain-name-or-IPv4-address[:port-number]</pre> <p>To use IPv6, specify a fully qualified domain name.</p> <p>To use a port number other than 25, you must specify the port number.</p> <pre>mailtoaddress=email-recipient-address</pre> <p>Up to four addresses can be specified. When specifying multiple addresses, separate the addresses with commas (,).</p> <pre>mailfromaddress=email-sender-address replytoaddress=reply-destination-address-(optional)</pre>

Item	Description
	<p>messagelevel=<i>message-level- (optional)</i></p> <p>Specify 1 to send email notifications about errors and higher-level (fatal error) problems. Specify 2 to send email notifications about warnings and higher-level (error and fatal error) problems. 2 is the default.</p> <p>Specify email addresses in the format <i>user-name@domain-name</i>.</p> <p>If a hash mark (#) is placed at the beginning of a line, the line is treated as a comment. Use hash marks to disable definitions.</p>
Settings	Edit the selected system file.
#1:	IP addresses specified in IPv6 format must be enclosed in square brackets ([]).

```

...
#####
# Access Control
#####
...
####
# First, map the community name (COMMUNITY) into a security name
# (local and mynetwork, depending on where the request is coming
# from):

#      sec.name source      community
com2sec SecNameDef1 localhost stdDefComm1
com2sec6 SecNameDef1 default  stdDefComm1

####
# Second, map the security names into group names:

#      sec.model sec.name
group GroupDef1 v1      SecNameDef1
group GroupDef1 v2c     SecNameDef1
group GroupDef1 usm     SecNameDef1
group snmpv3group usm user1

####
# Third, create a view for us to let the groups have rights to:

#      incl/excl subtree      mask
view ViewDef1 included .1      80
view snmpv3view included .1.3.6.1.2.1.1 fe

####
# Finally, grant the 2 groups access to the 1 view with different
# write permissions:

#      context sec.model sec.level match read write notif
access GroupDef1 "" any noauth exact ViewDef1 none none
access snmpv3group "" any priv exact snmpv3view none none

...
#####
# Further Information
#
# See the snmpd.conf manual page, and the output of "snmpd -H".
# MUCH more can be done with the snmpd.conf than is shown as an
# example here.
router user1 priv
createUser user1 MD5 mypassphrase DES mypassword

```

Note: Red frames indicate the parts edited or added for use of SNMPv3.

Example C-1 Example of specifying the settings in the snmpd.conf file when using SNMPv3

Performance Tuning page

A system administrator can tune the system performance.



Note: The system administrator can change the buffer cache settings to adjust system performance. However, this is not necessary for normal operation. If you want to tune the system performance, contact our Technical Support Center.

To display the **Performance Tuning** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **Performance Tuning** button.

Table C-114 Items displayed on the Performance Tuning page

Item		Description
Buffer flush daemon control	Percentage of buffer cache dirty to activate bdflush	Specify the level of dirty cache at which to start flushing the buffer cache (units: %). Set a number from 0 to 100.
	Jiffies delay between kupdate flushes	Specify the interval between buffer cache flushes (units: 10 ms). Set a number from 1 to 1000000. We recommend that you specify a number that is not greater than 60000.
	Time for normal buffer to age before we flush it	Specify the grace period before starting to flush the buffer (units: 10 ms). Set a number from 100 to 600000.
	Percentage of buffer cache dirty to activate bdflush synchronously	Specify the level of dirty cache at which to start an urgent buffer flush process (units: %). Set a number from 0 to 100. Note that this setting activates the flush process if the dirty cache percentage is reached before the grace period expires.
Minimum count of i-nodes resident in the cache		Specify the minimum number of inodes that are to be resident in the buffer cache. Set a number from 0 to 50000000.
Time for buffer to age before we flush it		Specify a grace period before starting to flush the metadata buffer cache (units: 10 ms). Set a number from 100 to 720000.
Interval between runs of the delayed write flush daemon		Specify the interval at which the write-delayed metadata buffer cache is flushed (units: 10 ms). Set a number from 50 to 3000.

List of SNMPS page

You can view the SNMP information.

To display the **List of SNMPS** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **SNMP Setup** button.

Table C-115 Items displayed on the List of SNMPs page

Item	Description
Source	Displays the server name and IP address of the SNMP manager.
Number of MIB objects	Displays the number of MIB objects.
Edit button	Click to edit the SNMP information. Use a radio button to select the SNMP information you want to edit, and then click this button. The Edit SNMP page opens (Edit SNMP page on page C-135).
Delete button	Click to delete the SNMP information. Use a radio button to select the SNMP information you want to delete, and then click this button.
Add button	Click to add SNMP information. The Add SNMP page opens (Add SNMP page on page C-136).

Edit SNMP page

You can change the SNMP information.

For details on the values that can be specified for each item, see the **Add SNMP** page ([Add SNMP page on page C-136](#)).



Note: To obtain system operating information or use SNMP trap notifications when you are using SNMPv2 in an IPv6 environment or SNMPv3, you must edit the `snmpd.conf` file in the **Edit System File** page (see subsection [Edit System File page on page C-126](#)).

To display the **Edit SNMP** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **SNMP Setup** button. Then, on the **List of SNMPs** page, select the radio button for the SNMP information you want to change, and then click the **Edit** button.

Table C-116 Items displayed on the Edit SNMP page

Item	Description
Source	Specify the server name and IP address of the SNMP manager. The specified source SNMP manager can view and acquire information from the MIB object.
Community	Specify a community name. The SNMP manager uses the community name to access the MIB value of an SNMP agent.
MIB objects	Specify the MIB object name, the mask, and the specification method. List of selectable MIB objects (MIB object name, Mask, How to specify) Select the name of the MIB object to be added to the SNMP configuration file, the mask, and the specification method. Text box

Item	Description
	<p>The name and mask for the MIB object selected in List of selectable MIB objects (MIB object name, Mask, How to specify) are shown.</p> <p>Drop-down list</p> <p>Select whether to include or exclude subtrees of the MIB object displayed in the text box.</p>

Add SNMP page

You can add SNMP information.



Note:

- The maximum number of SNMP information items is 128.
- To obtain system operating information or use SNMP trap notifications when you are using SNMPv2 in an IPv6 environment or SNMPv3, you must edit the `snmpd.conf` file in the **Edit System File** page (see subsection [Edit System File page on page C-126](#)).

To display the **Add SNMP** page, select **system** from the drop-down list on the **System Setup Menu** page, click the **Display** button, and then click the **SNMP Setup** button. Then, click the **Add** button on the **List of SNMPs** page.

Table C-117 Items displayed on the Add SNMP page

Item	Description
Source	<p>Specify the server name or IPv4 IP address of the SNMP manager permitted to access MIB information.</p> <p>By default, the settings are specified so that all hosts in the network are able to access MIB objects. To limit MIB object access to only specified SNMP managers, delete all entries specified by default, and then add the local host settings (<code>localhost</code>)# to display the local host setting on the top of the List of SNMPs page. Then, specify the SNMP manager or managers that are permitted to access MIB objects.</p>
Community	<p>Specify a community name using no more than 32 characters.</p> <p>The SNMP manager uses the community name to access the MIB value of an SNMP agent.</p> <p>You can specify ASCII alphanumeric characters and the following ASCII symbols:</p> <p>! # \$ % & ' () * + , - . / ; < = > ? @ [\] ^ _ ` { } ~</p> <p>A hash mark (#) cannot be used for the first character of a community name.</p> <p>If you use a backslash (\) or single quotation mark ('), insert a backslash as an escape character before the character that you want to use.</p> <p>The characters that can be used when specifying this community name are different from those that can be used when specifying the community name to be used when sending SNMPv2 traps. If you want to use the same community name as the one used when sending</p>

Item	Description
	SNMPv2 traps, specify the community name that you specified in Table C-113 Items displayed on the Edit System File page on page C-127 .
MIB objects	<p>Specify the MIB objects that can be obtained by the SNMP manager specified for Source.</p> <p>In the two text boxes above the Select button, specify the OID and mask for the MIB object. Then, in the drop-down list, select Include if you want to include subtrees of the OID, or select Do not include if you do not want to do so. Click the Select button to add the entries to the List of selectable MIB objects (MIB object name, Mask, How to specify) field and Selected MIB objects field.</p> <p>To delete an unnecessary entry, select the target MIB object from Selected MIB objects, and then click the Delete button.</p> <p>For details about the MIB objects to be specified, see section MIB objects for responding to SNMP get requests on page F-3.</p>
	<p>#: When you add local host settings, specify as follows:</p> <ul style="list-style-type: none"> • Source: localhost • Community: stdDefComm1 • MIB objects <ul style="list-style-type: none"> ◦ the OID of the MIB object: .1 ◦ the mask: 80 ◦ the drop-down list: Include

Access Protocol Configuration dialog box

You can perform operations such as changing the client authentication method.

To display the **Access Protocol Configuration** dialog box, click **Access Protocol Configuration** in the **Settings** area of the *host-name* window.

List of Services page

You can set up CIFS, NFS, FTP, and SFTP services.

The **List of Services** page first appears after the **Access Protocol Configuration** dialog box is displayed.

Table C-118 Items displayed on the List of Services page

Item	Description
Service name	<p>Displays the service name.</p> <p>CIFS</p> <p>Displayed when the service is a CIFS service.</p> <p>FTP</p> <p>Displayed when the service is an FTP service.</p> <p>NFS</p>

Item	Description
	<p>Displayed when the service is an NFS service.</p> <p>SFTP</p> <p>Displayed when the service is an SFTP service.</p> <p>SSH</p> <p>Displayed when the service is an SSH service.</p>
Status	<p>Displays the operating status of the service.</p> <p>Running</p> <p>Displayed when the service is running normally.</p> <p>Down</p> <p>Displayed when the service is running in an incomplete state.</p> <p>Offline</p> <p>Displayed when the resource group is offline.</p> <p>Stopped</p> <p>Displayed when the service has stopped.</p>
Automatic startup	<p>Displays the setting whether to automatically start the service when the node starts or restarts.</p> <p>On</p> <p>Displayed when automatic startup is set for the service.</p> <p>Off</p> <p>Displayed when automatic startup is not set for the service.</p>
Information	<p>This item is displayed when the service needs to be restarted or started.</p> <p>The configuration has been modified. Make sure the file system has been unmounted from the NFS client, and then restart the service. Rebooting the OS will not apply the changes.</p> <p>This message is displayed if the service was not restarted after the configuration definition of the NFS service was modified. Make sure that the file system has been unmounted from the NFS client, and then restart the service. Rebooting the node will not apply the changes.</p> <p>The configuration has been modified. Make sure the file system has been unmounted from the NFS client, and then start the service. Rebooting the OS will not apply the changes.</p> <p>This message is displayed if the service has remained stopped since the configuration definition of the NFS service was modified. Make sure that the file system has been unmounted from the NFS client, and then start the service. Rebooting the node will not apply the changes.</p> <p>The configuration has been modified. Restart the service. Rebooting the OS will not apply the changes.</p> <p>This message is displayed if the service was not restarted after the configuration definition of the NFS service, CIFS service, FTP service, or SFTP service was modified or the LDAP server settings were modified. Restart the service. Rebooting the node will not apply the changes.</p>

Item	Description
	<p>The configuration has been modified. Start the service. Rebooting the OS will not apply the changes.</p> <p>This message is displayed if the service has remained stopped since the configuration definition of the NFS service, CIFS service, FTP service, or SFTP service was modified or the LDAP server settings were modified. Start the service. Rebooting the node will not apply the changes.</p> <p>The service is incomplete. Restart the service.</p> <p>This message appears if the service is running in an incomplete state. If this message appears, restart the service because a problem might have occurred. If the message continues to be displayed after the restart, collect error information and contact maintenance personnel.</p>
Stop button	<p>Stops the CIFS, NFS, FTP, or SFTP service.</p> <p>Note:</p> <p>Contact clients before stopping the services.</p>
Start button	<p>Starts the CIFS, NFS, FTP, or SFTP service.</p> <p>Note:</p> <p>If you start the NFS service in an environment where the CIFS service and the NFS service share a directory, accessing a file system from the CIFS client might fail. If this happens, wait a while, and then try to access the file system again.</p>
Restart button	<p>Restarts the CIFS, NFS, FTP, or SFTP service.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Contact clients before stopping the services. • After modifying the configuration definitions for the NFS, CIFS, FTP, or SFTP services, the system administrator must restart these services to apply the changes. For details about the operations that require services to be restarted, see The description of the operations that require services to be restarted on page C-140. • If you start the NFS service in an environment where the CIFS service and the NFS service share a directory, accessing a file system from the CIFS client might fail. If this happens, wait a while, and then try to access the file system again.
Change Startup Setting button	<p>Changes the automatic restart setting for the CIFS, NFS, FTP, or SFTP service.</p>
Modify Configuration button	<p>Changes the configuration definition of a service.</p> <p>Selecting a service and then clicking this button displays a page where you can change the configuration definition for the selected service.</p>
Service Maintenance button	<p>Click this button if one of the items below applies. Clicking this button displays the CIFS Service Maintenance page (CIFS Service Maintenance page on page C-177).</p> <ul style="list-style-type: none"> • You want to view the configuration definition for a CIFS service • You want to delete cached user mapping information • You want to rejoin a node to an Active Directory domain

The description of the operations that require services to be restarted

After modifying the configuration definitions for the services, the services must be restarted. In addition, the following operations require services to be restarted.

If the following operations are performed, the NFS service must be restarted.

- When both the Active Directory domain controller and the KDC server are used as one server, if a name that is different from the domain name that belongs to the KDC server used by the NFS service or from the name of the KDC server is specified for the **Domain name** or **DC server name(s)** in the **Active Directory Authentication** page of the **Access Protocol Configuration** dialog box
- When editing the `/etc/hosts` file or the `/etc/cifs/lmhosts` file on the **Edit System File** page of the **Network & System Configuration** dialog box
- When specifying actions to respond to the delay time of the network environment by using the `nfsoptset` command
- When changing the port number allocation method for the NFS service by using the `nfssvset` command

If the following operations are performed, the CIFS service must be restarted.

- When using a command to modify the CIFS share settings while the CIFS service configuration definition settings do not allow the CIFS share settings to be automatically reloaded
- If the real-time scanning is enabled or disabled
After you enable or disable the real-time scanning, restart the CIFS service.
- When modifying the settings for the **Cache size of the scanning result** on the **Scan Conditions** page of the **Virus Scan Server Configuration** dialog box while real-time scanning is enabled
Disable real-time scanning, re-enable it, and then restart the CIFS service.
- When editing the `/etc/hosts` file or the `/etc/cifs/lmhosts` file on the **Edit System File** page of the **Network & System Configuration** dialog box
The modified settings will be applied 11 minutes after the file is edited. If you want the new settings to be applied immediately, restart the CIFS service.
- When both the Active Directory domain controller and the KDC server are used as one server, if a name that is different from the Active Directory domain name used by the CIFS service or from the name of the domain controller is specified for the **Domain name** or **KDC server name(s)** in the **NFS Service Management** page of the **Access Protocol Configuration** dialog box

If the following operations are performed, the FTP or SFTP service must be restarted.

- If the FTP or SFTP service settings allow users authenticated with Active Directory to log on, and the authentication type is changed from Active Directory to another type or from another type to Active Directory.
- When modifying the settings for the **LDAP setup (for user authentication)** on the **DNS, NIS, LDAP Setup** page of the **Network & System Configuration** dialog box

CIFS Service Management (Basic) page

You can change the basic settings of the CIFS service configuration definition.



Note:

- If the system administrator changes the configuration definition of the CIFS service while a CIFS client is updating the file system, the CIFS client operation might not be completed normally. The system administrator must inform users beforehand that the configuration definition will be changed.
- After changing the settings, restart the service to apply the new configuration definition.
- If you want to perform user mapping using LDAP, after changing the settings, use the **Check for Errors** dialog box to display the **List of RAS Information** page (for *Server check*), and then confirm that the LDAP server has been set up correctly.

To display the **CIFS Service Management (Basic)** page, select **CIFS** for **Service name** in the **List of Services** page, and then click the **Modify Configuration** button.

Table C-119 Items displayed on the CIFS Service Management (Basic) page

Item		Description
Setting Type drop-down list		Specify the type of information to be specified or changed. Basic: The basic information related to the CIFS service configuration definition is specified. User mapping: User mapping is specified. Security: Changes the settings related to CIFS service security. Performance: Changes the settings related to CIFS service performance. Administration: Changes the settings for the CIFS administrators.
Display button		Displays the information.
CIFS service setup	SMB protocol	Specify the SMB protocol to be used for accessing from the CIFS client. SMB 1.0

Item	Description
	<p>Select this option if you use SMB 1.0.</p> <p>SMB 2.0</p> <p>Select this option if you use SMB 2.0. SMB 1.0 can also be used.</p> <p>SMB 2.1</p> <p>Select this option if you use SMB 2.1. SMB 1.0 and SMB 2.0 can also be used.</p> <p>SMB 3.0</p> <p>Select this option if you use SMB 3.0. SMB 1.0, SMB 2.0, and SMB 2.1 can also be used.</p> <p>If you modify the setting from SMB 3.0, when you have set the CIFS service to encrypt the communication with the CIFS client, the client might not access the share. Review the encryption settings on the CIFS Service Management (Security) page and in the Edit Share dialog box.</p> <p>If you change this setting when real-time scanning by using Trend Micro ServerProtect is enabled, you need to restart the OS on the scanning server.</p>
Server comment	<p>Enter a comment for the server name that appears on the CIFS client.</p> <p>Enter a maximum of 256 characters. You can specify alphanumeric characters and the following symbols:</p> <p>! # \$ % & ' () * + , . / : < > ? @ [\] ^ _ ` { } ~</p> <p>You can also specify spaces, but not at the beginning or end of the character string. A backslash (\) cannot be used at the end of the entry. In addition, you can specify multi-byte characters.</p> <p>This item is optional.</p>
Authentication mode	<p>Displays the user authentication method used for the access from a CIFS client to the CIFS share.</p> <p>Local authentication</p> <p>Displayed when local authentication is used.</p> <p>NT domain authentication</p> <p>Displayed when NT domain authentication is used.</p> <p>Active Directory authentication</p> <p>Displayed when Active Directory authentication is used.</p>

Item		Description
CIFS default setup	Volume Shadow Copy Service	Specify whether to use Volume Shadow Copy Service to make past versions of files that have been migrated to an HCP system available to CIFS clients. Use Select this to use Volume Shadow Copy Service. Do not use Select this if you do not want to use Volume Shadow Copy Service.
Change Authentication Mode button		Changes the user authentication method. Clicking this button displays the Select Authentication Mode page (Select Authentication Mode page on page C-157).

CIFS Service Management (User mapping) page

User mapping can be specified, when the authentication mode that is specified for the CIFS service is either NT domain authentication or Active Directory authentication.

Select a radio button to choose whether to use user mapping, and specify the necessary information, depending on whether you use user mapping.

- When user mapping uses RIDs
- When user mapping uses LDAP
- When user mapping uses the Active Directory schema
- When user mapping is not used



Note: The following are notes on using user mapping:

- To change the user mapping method that you use, you need to re-create the file systems after you migrate the data by using Windows backup function.
- Once a user ID or group ID is assigned, it can no longer be reused, even if you delete the user information from the domain controller.



Note: Note the following when user mapping uses RIDs:

- Specify the range of user IDs and group IDs so that the range does not include user IDs and group IDs registered in the HDI system, on the NIS server, or on the LDAP server for user authentication.
- Even if a user registered on the domain controller is registered with the same name in the HDI system, on the NIS server, or on the LDAP server for user authentication, the user ID and group ID assigned by RID user mapping will be used when the user accesses a CIFS share.
- Considering that the range of user IDs and group IDs could be extended in the future for the HDI system, the NIS server, and the LDAP server for

user authentication, we recommend that you do not use user IDs and group IDs beyond the range set by user mapping.



Note: Note the following when user mapping uses LDAP:

- Information about assigned user IDs and group IDs is stored on the LDAP server as a database. You must create the tree for storing user IDs and group IDs on the LDAP server before restarting the CIFS server.
- Make sure that the user IDs and group IDs that you register on the LDAP server do not duplicate the user IDs and group IDs registered in the HDI system, on the NIS server, or on the LDAP server for user authentication. When you use automatic ID allocation, make sure that the ID range that you specify does not include a user ID or group ID registered in the HDI system, on the NIS server, or on the LDAP server for user authentication.
- Even if a user registered on the domain controller is registered with the same name in the HDI system, on the NIS server, or on the LDAP server for user authentication, the user ID and group ID assigned by LDAP user mapping will be used when the user accesses a CIFS share.
- When automatic ID allocation is used, the possibility that the range of user IDs and group IDs will be extended in the future for the HDI system, the NIS server, and the LDAP server for user authentication must be considered. We therefore recommend that you do not use user IDs and group IDs beyond the range set by user mapping.



Note: Note the following when user mapping uses the Active Directory schema:

- Use IDs from 200 to 2147483147 for user IDs and group IDs that you register in Active Directory.
- Make sure that the user IDs and group IDs that you register on the domain controller do not duplicate the user IDs and group IDs registered in the HDI system, on the NIS server, or on the LDAP server for user authentication.

To display the **CIFS Service Management (User mapping)** page, select **User mapping** from the drop-down list on any **CIFS Service Management** page, and then click the **Display** button.

Table C-120 Items displayed on the CIFS Service Management (User mapping) page

Item		Description	See
User mapping setup	Use user mapping using RIDs.	Select this item when you want user mapping to use RIDs.	Table C-121 Items specified when the Use user mapping using RIDs. is selected in User mapping setup on the CIFS Service Management (User mapping) page on page C-145

Item	Description	See
Use user mapping using LDAP.	Select this option when you want user mapping to use LDAP.	Table C-122 Items specified when the Use user mapping using LDAP. is selected in User mapping setup on the CIFS Service Management (User mapping) page on page C-147
Use user mapping using Active Directory schema.	Select this when user mapping uses the Active Directory schema.	Table C-124 Items specified when the Use user mapping using Active Directory schema. is selected in User mapping setup on the CIFS Service Management (User mapping) page on page C-149
Do not use user mapping.	Select this option if you do not want user mapping to be used. If the setting was changed to not use user mapping, after the service is applied, the range of user IDs and group IDs set before the change is still displayed in User mapping setup on the CIFS Service Management (User mapping) page. If user mapping used RIDs before the change, the range of user IDs and group IDs set for each domain is also displayed.	--

Table C-121 Items specified when the Use user mapping using RIDs. is selected in User mapping setup on the CIFS Service Management (User mapping) page

Item	Description
Range of UIDs and GIDs	<p>Specify a range of user IDs and group IDs to be used for user mapping. You can specify a range of IDs within the range from 70000 to 2147483147.</p> <p>Specify the minimum value in the left text box and the maximum value in the right text box.</p> <p>You cannot use the user IDs and group IDs that are being used by the HDI system, the NIS server, the LDAP server for user authentication, or another domain.</p> <p>When you extend the range of user IDs and group IDs set for user mapping after applying the service, make sure the user IDs and group IDs that are being used by the HDI system, the NIS server, the LDAP server for authentication, and another domain are not included in the</p>

Item	Description
	<p>new range, and then change the maximum value. If changing the maximum value would result in one or more of the currently used user IDs or group IDs being included in the new range, you need to re-create the file system, and then change the minimum value to extend the range.</p> <p>Set an adequate range of user IDs and group IDs after considering how long the operation will be performed and how much the number of users will increase.</p>
<p>Settings for each domain</p>	<p>Specify a range of user IDs and group IDs for each domain. You can specify a range for a maximum of 256 domains. Register no more than 20 domains each time. If more than 20 domains are registered at the same time, a timeout might occur.</p> <p>Register all domains that have been specified in the authentication mode. If you only register domains that have trust relationships, the users on those domains are not allowed access to the CIFS share.</p> <p>Domain name (NetBIOS)</p> <p>Specify a domain name.</p> <p>Specify the name of a domain that has been specified in the authentication mode or a domain that has a trust relationship.</p> <p>Range of UIDs and GIDs</p> <p>Specify a range of user IDs and group IDs for the specified domain. You can specify this range within the range of user IDs and group IDs set by user mapping.</p> <p>Specify the minimum value in the left text box and the maximum value in the right text box. Make sure that the range for a domain does not overlap the range of another domain. The ranges for domains do not need to be consecutive.</p> <p>After specifying the name of a domain and the range of user IDs and group IDs for the domain, when you click the Set button, the specified information is added to a list box. To remove an entry from the list box, select the entry and then click the Delete button. The entries in the list box are sorted in ascending order based on the ID range minimum value of each domain.</p> <p>You cannot use the user IDs and group IDs that are being used by the HDI system, the NIS server, the LDAP server for user authentication, or another domain.</p> <p>When you extend the range of user IDs and group IDs set for user mapping after applying the service, make sure the user IDs and group IDs that are being used by the HDI system, the LDAP server for authentication, the NIS server, and another domain are not included in the new range, and then change the maximum value. If changing the maximum value would result in one or more of the currently used user IDs or group IDs being included in the new range, you need to re-create the file system, and then change the minimum value to extend the range.</p> <p>Set an adequate range of user IDs and group IDs after considering how long the operation will be performed and how much the number of users will increase.</p>

Table C-122 Items specified when the Use user mapping using LDAP. is selected in User mapping setup on the CIFS Service Management (User mapping) page

Item	Description
LDAP server name	Specify the IP address or the host name of the LDAP server to be used for user mapping (the IP address is recommended).
LDAP server port number	Specify an LDAP server port number in the range from 1 to 65535. This item is optional. The default value is 389.
LDAP server root DN	Specify the identification name of the LDAP server root in DN format, as in the following example: <code>dc=hitachi,dc=co,dc=jp</code>
LDAP user map DN	Specify in DN format the identification name for which you want to add an LDAP server user mapping account. Specify only the relative DN from LDAP server root DN , as in the following example: <code>ou=idmap</code> This item is optional. If you omit this item, the user mapping account is stored in the DN specified in LDAP server root DN .
LDAP administrator DN	Specify the identification name of the LDAP server administrator in DN format. Specify only the relative DN from LDAP server root DN , as in the following example: <code>cn=Administrator</code>
LDAP administrator password	Specify the LDAP administrator password.
Allocate automatically	<p>Select this to allocate user IDs and group IDs automatically.</p> <p>Range of UIDs</p> <p>Specify a range of user IDs within the range from 70000 to 2147483147.</p> <p>Specify the minimum value in the left text box and the maximum value in the right text box.</p> <p>Range of GIDs</p> <p>Specify a range of group IDs within the range from 70000 to 2147483147.</p> <p>Specify the minimum value in the left text box and the maximum value in the right text box.</p> <p>If multiple CIFS clients attempt to open different CIFS shares on multiple nodes concurrently by using the same name for a new domain user, an ID might be missing from the range specified by Range of UIDs and Range of GIDs. The ID will not be reused.</p> <p>When you extend the range of user IDs and group IDs set for user mapping after applying the service, make sure that user IDs and group IDs that are being used by the HDI system, the NIS server, or another domain are not included in the new range, and then change the maximum value. If changing the maximum value would result in one or more of the currently used user IDs or group IDs being included in the new range, you need to re-create the file system, and then change the minimum value to extend the range.</p>

Item	Description
	<p>If you change the minimum value of a previously set user ID or group ID, you need to perform additional tasks such as re-creating the LDAP server. Set an adequate range of user IDs and group IDs after considering how long the operation will be performed and how much the number of users will increase.</p> <p>When user mapping uses LDAP and assigns IDs automatically, you can check the largest value of the assigned user IDs and group IDs in User mapping ID assignment information on the CIFS Service Management (User mapping) page.</p>
Allocate manually	<p>Select this to allocate user IDs and group IDs manually.</p> <p>Use IDs from 200 to 2147483147 for user IDs and group IDs that you register on the LDAP server.</p> <p>In Table C-123 Items displayed in the User mapping ID assignment information on the CIFS Service Management (User mapping) page on page C-148, you can check the largest ID within the range of user IDs and group IDs that have already been assigned in the HDI system.</p>

Table C-123 Items displayed in the User mapping ID assignment information on the CIFS Service Management (User mapping) page

Item	Description
Largest currently used UID	<p>Displays the largest user ID within the range of user IDs that have already been assigned in the HDI system. Depending on the status of user mapping usage, the following information might be displayed:</p> <p>-</p> <p>Displayed when user mapping is not used.</p> <p>Not used, or less than the minimum UID used.</p> <p>Displayed when no user IDs have been assigned, or the smallest assigned user ID is smaller than the minimum value set in Range of UIDs.</p> <p>Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.</p> <p>Displayed when the largest user ID could not be acquired from the LDAP server for user mapping. Check the user mapping settings and the operating status of the LDAP server.</p>
Largest currently used GID	<p>Displays the largest group ID within the range of group IDs that have already been assigned in the HDI system. Depending on the status of user mapping usage, the following information might be displayed:</p> <p>-</p> <p>Displayed when user mapping is not used.</p> <p>Not used, or less than the minimum GID used.</p> <p>Displayed when no group IDs have been assigned, or the smallest assigned group ID is smaller than the minimum value set in Range of GIDs.</p> <p>Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.</p>

Item	Description
	Displayed when the largest group ID could not be acquired from the LDAP server for user mapping. Check the user mapping settings and the operating status of the LDAP server.

Table C-124 Items specified when the Use user mapping using Active Directory schema. is selected in User mapping setup on the CIFS Service Management (User mapping) page

Item	Description
Name service switch	Select the name service switch. Select Using LDAP as a network information service (RFC2307) . Microsoft® Services for Unix Select this to use Microsoft services for Unix to obtain user IDs and group IDs from the domain controller. Using LDAP as a network information service (RFC2307) Select this to use the RFC2307 schema to obtain user IDs and group IDs from the domain controller.
Joined domain name	Displays the name of the domain to which nodes belong.
Trusted domain name	Displays the name of a domain that has a confidential relationship with the domain to which nodes belong. If there is no domain that has a confidential relationship, - is displayed.
<p>Note: Use IDs from 200 to 2147483147 for user IDs and group IDs that you register in Active Directory.</p> <p>If Domain controller: LDAP server signing requirements of the domain controller policy is Require signing, startup of the CIFS services will fail. Therefore, select None.</p> <p>For checking the domain controller policy, choose Administrative Tools, Group Policy Management Editor, Computer Configuration, Policies, Windows Settings, and then Security Settings. In the window that appears, choose Local Policies and then Security Options, and then check whether Domain controller: LDAP server signing requirements is specified.</p>	

CIFS Service Management (Security) page

You can change the CIFS service security settings.



Note:

- If the system administrator changes the configuration definition of the CIFS service while a CIFS client is updating the file system, the CIFS client operation might not be completed normally. The system administrator must inform users beforehand that the configuration definition will be changed.
- After changing the settings, restart the service to apply the new configuration definition.

To display the **CIFS Service Management (Security)** page, select **Security** from the drop-down list on any **CIFS Service Management** page, and then click the **Display** button.

Table C-125 Items displayed on the CIFS Service Management (Security) page

Item		Description
CIFS service setup	Host access restrictions	<p>To limit the CIFS clients that can access the CIFS share, specify, in the text box, the host name or IP address of each CIFS client that is to be allowed access to the CIFS share. Alternatively, specify the network address of the network to which each CIFS client belongs. To specify multiple CIFS clients, delimit clients by using commas (,). Note that you can specify no more than 5,631 characters in total. To allow all CIFS clients access to the CIFS share, do not specify anything in the text box.</p> <p>You must also select an option to specify whether the specified CIFS clients are to be allowed or denied access to the CIFS share.</p> <p>Allow</p> <p>Allows the specified hosts or networks to access the nodes.</p> <p>Deny</p> <p>Does not allow the specified hosts or networks to access the nodes.</p> <p>User authentication is performed for a CIFS client even if access to the nodes is permitted.</p> <p>When you specify a host name, on the Edit System File page, edit the <code>/etc/hosts</code> file to add the names and IP addresses of all hosts that are specified in Host access restrictions. If the host names are not added to the <code>/etc/hosts</code> file, the information specified here might not take effect. If you specify a host name that corresponds to an IP address and that has been added as an alias after the first host name, the system might not work properly.</p> <p>You cannot specify the following names as the host name:</p> <ul style="list-style-type: none"> • ALL • FAIL • EXCEPT <p>Specify the network address in the format below: <i>network-address/netmask</i> (example: 10.203.15.0/255.255.255.0)</p> <p>Specify a prefix length for the netmask for IPv6.</p>
	Mapping to guest account	<p>Specify the definition of guest account users.</p> <p>Unregistered users</p> <p>Select this if users unregistered in the system can be guest account users.</p>

Item	Description
	<p>Unregistered users or invalid passwords</p> <p>Select this if users unregistered in the system or users registered in the system who use an incorrect password can be guest account users.</p> <p>Note that if Unregistered users or invalid passwords is selected, users registered in the system can be guest account users even if the users enter an incorrect password.</p> <p>Never</p> <p>Select this to deny access by guest account users to the CIFS shares.</p> <p>The guest account is regarded as <i>nobody</i> (user ID: 65534). Therefore, allow access permissions in the CIFS share that guest account users can access as <i>nobody</i>. You cannot set an ACL that specifies a guest account.</p> <p>The users unregistered in the system differ depending on the user authentication mode being used, as shown below.</p> <ul style="list-style-type: none"> • When Local authentication is being used The users not registered in the HDI system • When NT domain authentication is being used The users not registered in the domain controller in the domain • When Active Directory authentication is being used The users not registered in the Active Directory domain controller
NetBIOS over TCP/IP	<p>Specify whether to accept access from CIFS clients that uses NetBIOS over TCP/IP.</p> <p>Use</p> <p>Select this if you want the CIFS service to accept access from CIFS clients that uses NetBIOS over TCP/IP.</p> <p>If Use is selected, name resolution that uses WINS, lmhosts, or broadcast, and the browsing function are available. When using the browsing function for CIFS shares, configure the network required to use CIFS shares as described in the <i>Installation and Configuration Guide</i>.</p> <p>Do not use</p> <p>Select this if you do not want the CIFS service to accept access from CIFS clients that uses NetBIOS over TCP/IP.</p> <p>If Do not use is selected, the load of data communication and the security risks can be reduced. However, note that the available name resolution services are only for DNS or hosts. The browsing function is not available.</p>
CIFS access log	Specify whether to collect CIFS access log data.

Item		Description
		<p>Use</p> <p>Select this if you want to collect CIFS access log data.</p> <p>Select If the CIFS access log file exceeds the max. size, do not collect log data. if the log file cannot be moved (when the move destination is not specified, or when the capacity of the file system to which the log file is to be moved has reached the maximum limit), and if you want to stop collecting CIFS access log data when the capacity of the log file reaches the maximum limit. You can select If the CIFS access log file exceeds the max. size, do not collect log data. only when Use is selected.</p> <p>Do not use</p> <p>Select this if you do not want to collect CIFS access log data.</p>
CIFS default setup	Guest account access	<p>For CIFS shares, specify access permissions for guest account users.</p> <p>Allow</p> <p>Select this to allow guest account users access to the CIFS service.</p> <p>Disallow</p> <p>Select this to disallow guest account users access to the CIFS service.</p> <p>The guest account is regarded as <i>nobody</i> (user ID: 65534). Therefore, allow access permissions in the CIFS share that guest account users can access as <i>nobody</i>. You cannot set an ACL that specifies a guest account.</p>
	Access Based Enumeration	<p>Specify whether to use access-based enumeration.</p> <p>Use</p> <p>Select this to use access-based enumeration.</p> <p>Do not use</p> <p>Select this to not use access-based enumeration.</p>
	File timestamp changeable users	<p>Select the users for whom you want to allow updating of CIFS share file timestamps. Select Write permitted users if the file is shared by the CIFS service only.</p> <p>Write permitted users</p> <p>Select this if you want to permit updating of the CIFS share file timestamp for all users who are permitted to write to this file.</p> <p>Owner only</p> <p>Select this if you want to restrict timestamp updating to the file owner.</p> <p>Note that this setting is invalid in an advanced ACL file system.</p>

Item	Description
Events logged to the CIFS access log	Specify the trigger conditions for collecting CIFS access log information. This setting is enabled only when Use is selected in CIFS access log . Clicking the Set Up button displays the Setting Events Logged to the CIFS Access Log page (Setting Events Logged to the CIFS Access Log page on page C-161).
SMB encryption	Specify whether communication with the CIFS client is to be encrypted. The setting for this item is only valid if you select SMB 3.0 for the SMB protocol in CIFS Service Management (Basic) page. If you select an option other than SMB 3.0 for the SMB protocol , select Disable . Auto Select this option if communication with the client is to be encrypted only when the client supports encryption. Mandatory Select this option if communication with the client is always to be encrypted. Only clients that support SMB 3.0 or later can access a CIFS share. Note that clients cannot access a CIFS share by using guest accounts. Disable Select this option if communication with the client is not to be encrypted.

CIFS Service Management (Performance) page

You can change the CIFS service performance settings.



Note:

- If the system administrator changes the configuration definition of the CIFS service while a CIFS client is updating the file system, the CIFS client operation might not be completed normally. The system administrator must inform users beforehand that the configuration definition will be changed.
- After changing the settings, restart the service to apply the new configuration definition.

To display the **CIFS Service Management (Performance)** page, select **Performance** from the drop-down list on any **CIFS Service Management** page, and then click the **Display** button.

Table C-126 Items displayed on the CIFS Service Management (Performance) page

Item	Description
CIFS service setup	<p>Client time-out</p> <p>Specify in minutes the maximum time to wait for a CIFS client response as the timeout value.</p> <p>Specify a value from 0 to 1440.</p> <p>When 0 is specified, a client is not automatically disconnected by a timeout. If the specified value is smaller than the default, reconnection attempts initiated by the client increase as smaller values are specified, and there are conflicts between processing of disconnections due to timeouts and processing of connections initiated by clients. Therefore, attempts to connect to the file system may fail depending on the number of CIFS clients or the operational status of nodes. In this case, you need to wait a while, and then connect from the CIFS client again.</p>
	<p>Automatic reloading of CIFS share settings</p> <p>Specify whether to reload the CIFS share settings automatically when they are changed.</p> <p>Perform</p> <p>Select this if you want to reload the CIFS share settings automatically.</p> <p>The CIFS share settings are automatically applied to the CIFS client environment when they are changed.</p> <p>Do not perform</p> <p>Select this if you do not want to reload the CIFS share settings automatically.</p> <p>If you select Perform, see the <i>File System Protocols (CIFS/NFS) Administrator's Guide</i> for details on the CIFS share settings that will be automatically reloaded.</p> <p>If you select Do not perform, take one of the following actions to apply the new CIFS share settings:</p> <ul style="list-style-type: none"> • Restart the CIFS service. • Log on to the CIFS client computers again. • End all connections from the CIFS client computers to the CIFS share, and then reconnect to the CIFS share. <p>However, even if you log on again to the CIFS client machine, or disconnect all the connections to the CIFS share from the CIFS client machines and then connect again, changes made to the CIFS share settings might not be applied to the client environment. If the changes are not applied, restart the CIFS service.</p> <p>Note that, this setting change also takes effect when the CIFS clients reconnect to the CIFS share after the connections to the CIFS share are automatically disconnected due to a timeout. When you select Do not perform, we recommend that you specify a small value (about 6 minutes) for Client time-out.</p>

Item		Description
CIFS default setup	Disk synchronization policy	<p>Specify the operations for write requests from CIFS clients to CIFS shares.</p> <p>At write and close</p> <p>Select this to write synchronously with a write request or a close request.</p> <p>At close</p> <p>Select this to write synchronously with a close request.</p> <p>Routine disk flush only</p> <p>Select this to write at a fixed interval, regardless of when write requests and close requests are made.</p>
	Windows® client access policy	<p>Select the method for processing I/O requests from Windows clients.</p> <p>Parallel</p> <p>Select this to asynchronously process I/O requests from Windows clients.</p> <p>Serial</p> <p>Select this to synchronously process I/O requests from Windows clients.</p>
	CIFS client cache	<p>Specify whether the updated data in the CIFS share file is to be cached on the client.</p> <p>If Use is selected, performance improves when the updated data in the CIFS share file is cached on the client. However, if an error occurs on the network or CIFS client, data reliability might deteriorate.</p> <p>Specify Do not use for read-write-content-sharing file systems. If the updated data of the file in the CIFS share is cached on the client, the update date might not be reflected properly on other sites.</p> <p>Note that, if you enable SMB encryption for a CIFS share, the updated data will not be cached, regardless of the value of this setting.</p> <p>Use</p> <p>Select this if the updated data in the CIFS share file is to be cached on the client.</p> <p>For the file systems listed below, we recommend also setting Read-only client cache for access conflicts values to Use, because there is a risk that the client cache will fail to validate.</p> <ul style="list-style-type: none"> - File systems that migrate data to an HCP system <p>Do not use</p> <p>Select this if the updated data in the CIFS share file is not to be cached on the client.</p>
	Read-only client cache for access conflicts	<p>Specify whether to use the read-only client cache when a file access contention occurs among CIFS clients.</p>

Item	Description
	<p>You can improve performance by selecting Use because data is cached on client machines when CIFS clients open a file.</p> <p>Use</p> <p>Select this to use the read-only client cache. You can specify this only when Use is selected for CIFS client cache.</p> <p>Do not use</p> <p>Select this if you do not want to use the read-only client cache.</p> <p>Note that we recommend that you do not use the read-only client cache if you also want to use the NFS protocol to access the file shares because changes might not be applied. If you need to use the read-only client cache, we recommend implementing file sharing individually for each protocol to ensure that the NFS protocol is not used to access the share.</p>

CIFS Service Management (Administration) page

You can change the CIFS administrator settings.



Note:

- If the system administrator changes the configuration definition of the CIFS service while a CIFS client is updating the file system, the CIFS client operation might not be completed normally. The system administrator must inform users beforehand that the configuration definition will be changed.
- After changing the settings, restart the service to apply the new configuration definition.

To display the **CIFS Service Management (Administration)** page, select **Administration** from the drop-down list on any **CIFS Service Management** page, and then click the **Display** button.

Table C-127 Items displayed on the CIFS Service Management (Administration) page

Item	Description
CIFS service setup CIFS administrator name(s)	<p>Specify a user name or a group name to be defined as a CIFS administrator.</p> <p>A CIFS administrator can perform operations such as deleting the unnecessary CIFS share files and changing permissions for all files and folders. If you want to specify multiple user names or group names, separate them by commas (,).</p> <p>Specify group names in the format <i>@group-name</i>.</p>

Item	Description
	<p>When you are using user mapping, specify a domain name with the user name or the group name as follows:</p> <p><i>domain-name\user-name</i> <i>@domain-name\group-name</i></p> <p>If you use the Active Directory authentication, specify the same domain name as specified in Domain name (NetBIOS).</p>

Select Authentication Mode page

A system administrator can set user authentication mode in the **Select Authentication Mode** page.

To display the **Select Authentication Mode** page, click the **Change Authentication Mode** button on the **CIFS Service Management (Basic)** page.

Table C-128 Items displayed on the Select Authentication Mode page

Item	Description
Authentication mode	<p>Select the method for authenticating users accessing the CIFS share from CIFS clients.</p> <p>Local authentication</p> <p>Select this to use local authentication. Local authentication uses the CIFS server function implemented in the node OS to authenticate users. When this item is selected, clicking the OK button displays the Local Authentication page (Local Authentication page on page C-158).</p> <p>NT domain authentication</p> <p>Select this to use NT domain authentication when IPv4 is used. NT domain authentication authenticates users with the domain controller in the domain. Users who are authenticated locally in an HDI system cannot access CIFS shares, because users are managed by the corresponding domain controller.</p> <p>If you set that user mapping is not to be used, the user information registered on the domain controller needs to be registered in the HDI system, on the NIS server, or on the LDAP server used for user authentication. For this reason, we recommend that you use user mapping when authenticating users by NT domain authentication.</p> <p>When this item is selected, clicking the OK button displays the NT Domain Authentication page (NT Domain Authentication page on page C-158).</p> <p>Active Directory authentication</p> <p>Select this to use Active Directory authentication. Active Directory authentication uses the Active Directory domain controller to authenticate users. Users who are authenticated locally in an HDI system cannot access CIFS shares, because users are managed by the Active Directory domain controller.</p>

Item	Description
	<p>If you set that user mapping is not to be used, the user information registered on the domain controller will need to be registered in the HDI system, on the NIS server, or on the LDAP server used for user authentication. For this reason, we recommend that you use user mapping when authenticating users by Active Directory authentication.</p> <p>When this item is selected, clicking the OK button displays the Active Directory Authentication page (Active Directory Authentication page on page C-159).</p>

Local Authentication page

A system administrator can set local authentication in the **Local Authentication** page.

To display the **Local Authentication** page, select **Local authentication** for **Authentication mode** on the **Select Authentication Mode** page, and then click the **OK** button.

Table C-129 Items displayed on the Local Authentication page

Item	Description
Workgroup name	<p>Enter the name of the work group to which the node belongs.</p> <p>Use a name that differs from the host name. If you specify the same name, the group name might not be displayed correctly when you set up an ACL.</p>

NT Domain Authentication page

A system administrator can set a NT domain authentication in the **NT Domain Authentication** page.

To display the **NT Domain Authentication** page, select **NT domain authentication** for **Authentication mode** on the **Select Authentication Mode** page, and then click the **OK** button.



Note:

- NT domain authentication can be used when IPv4 is used.
- If all the following conditions are satisfied, edit the `/etc/cifs/lmhosts` file to search the domain controllers in the domains that have a trust relationship with the domain to which the node belongs.
 - The domain to which the node belongs has a trust relationship with another domain.
 - The domain to which the node belongs or a domain that has a trust relationship with this domain is an NT domain.
 - The node is in a different network segment from a domain that has a trust relationship with the domain to which the node belongs.

- Make sure that there is no computer that satisfies all the following conditions on the network segment to which the node connects:
 - The name of the computer is the same as the domain controller server name specified on the **NT Domain Authentication** page.
 - The computer is not a server.
 To connect the node to multiple network segments (including VLANs), check the above conditions for all the network segments to which the node connects.
- To specify the server name of the domain controller, specify the computer name set to the domain controller. Do not specify another name (an alias name).

Table C-130 Items displayed on the NT Domain Authentication page

Item	Description
Domain name	Enter a domain name.
PDC server name	Enter the server name for the primary domain controller.
BDC server name	Enter the server name for the backup domain controller. This item is optional.
Domain administrator name	Enter the user name of the domain administrator.
Administrator password	Enter the password of the domain administrator.

Active Directory Authentication page

A system administrator can set active directory authentication in the **Active Directory Authentication** page.

To display the **Active Directory Authentication** page, select **Active Directory authentication** for **Authentication mode** on the **Select Authentication Mode** page, and then click the **OK** button.



Note:

- Make sure that the DNS server you are using in the Active Directory domain satisfies the following conditions:
 - The IP address of the node and the corresponding host name have been registered.
 - The SRV record that indicates the Active Directory service has been registered.
 - All the registered IP addresses corresponding to the host names of the domain controllers can be used for communication from the node.
 - IP addresses corresponding to the host names of the domain controllers are not dynamically added.
- When you change the Active Directory domain to which the node belongs, beware of the following:

- If you change the Active Directory domain and soon set the node to belong to the old Active Directory domain, authentication of CIFS clients might result in an error even if the processing finishes normally. On the **CIFS Service Maintenance** page, click the **Rejoin Active Directory Domain** button to add the node to the Active Directory domain again.
- If the node joins an Active Directory domain that is different from the old domain, but that has the same name as the old domain, unnecessary computer accounts might remain in the old Active Directory domain. If accounts remain, use the domain controller in the old Active Directory domain to delete the unnecessary computer accounts.
- If all the following conditions are satisfied, edit the `/etc/cifs/lmhosts` file to search the domain controllers in the domains that have a trust relationship with the domain to which the node belongs.
 - The domain to which the node belongs has a trust relationship with another domain.
 - The domain to which the node belongs or a domain that has a trust relationship with this domain is an NT domain.
 - The node is on a different network segment from a domain that has a trust relationship with the domain to which the node belongs.
- Try to maintain nearly the same time for the domain controller, the HDI system, and the CIFS clients. If the time differs by five minutes or more, authentication might fail when a CIFS client accesses the HDI system.
- If a user registered in the domain accesses the CIFS share provided by the HDI system from a client computer that is not registered in the domain, the user authentication might fail. If authentication fails, on the **CIFS Service Maintenance** page, check whether the NetBIOS name of the Active Directory domain has been set correctly.
- To specify the server name of the domain controller, specify the computer name set to the domain controller. Do not specify another name (an alias name).

Table C-131 Items displayed on the Active Directory Authentication page

Item	Description
Domain name	Enter the DNS name of the Active Directory domain. Any lower-case letters that are entered are treated as upper-case letters. <ul style="list-style-type: none"> • If both the Active Directory domain controller and the KDC server are used as one server: The name specified here will also be used as the name of the domain to which the KDC server belongs. • If, in the configuration definition of the NFS service, the domain name is set to be applied to the NFSv4 domain: The name specified here will also be used as the NFSv4 domain name. • When an FTP or SFTP service setting is used to determine whether users authenticated by Active Directory are permitted to log on:

Item	Description
	The name specified here will also be used as the domain name for the FTP or SFTP service.
Domain name(NetBIOS)	Enter the NetBIOS name of the Active Directory domain.
DC server name(s)	<p>Specify the server name for the Active Directory domain controller to which the nodes belong. You can also specify the IP address.</p> <p>Up to five server names can be specified. When specifying multiple names, separate each with a comma (,).</p> <ul style="list-style-type: none"> If both the Active Directory domain controller and the KDC server are used as one server: <p>The name specified here will also be used as the name of the KDC server.</p> When an FTP or SFTP service setting is used to determine whether users authenticated by Active Directory are permitted to log on: <p>The name specified here will also be used as the domain name for the FTP or SFTP service.</p>
Domain user name	<p>Specify the name of the Active Directory domain controller user. When specifying the name of the Active Directory domain controller user, keep the following points in mind:</p> <ul style="list-style-type: none"> If more than 10 servers are joined to the Active Directory domain, the user must belong to the <code>Account Operators</code> group. If you want to change the domain user, before changing the setting in the HDI system, delete the HDI account from the <code>Computers</code> container in the domain controller, or add a new domain user to the HDI account and give the following access permissions to the user: <ul style="list-style-type: none"> - Read - Validated write to DNS host name - Validated write to service principal name - Reset Password - Change Password - Write Account Restrictions
Domain user password	Enter the password of the user that is specified for Domain user name .

Setting Events Logged to the CIFS Access Log page

The **Setting Events Logged to the CIFS Access Log** page can be used to specify an event that triggers collection of the CIFS access log.

Specified settings are applied to the whole CIFS service. However, if events that trigger collection of the CIFS access log are specified for each CIFS share by using the `cifscreate` command or the `cifsedit` command, the settings for each CIFS share are given priority over the settings for the whole CIFS service. When the settings for the CIFS service are changed, check the

settings for each CIFS share as well as the settings for the whole CIFS service.

To display the **Setting Events Logged to the CIFS Access Log** page, click the **Set Up** button on **Events logged to the CIFS access log** from the **CIFS Service Management (Security)** page in the **Access Protocol Configuration** dialog box.

Table C-132 Items displayed on the Setting Events Logged to the CIFS Access Log page

Item	Description
Events logged to the CIFS access log	<p>Specify the events that trigger collection of the CIFS access log.</p> <p>Successful</p> <p>Select the check boxes for desired events (from the items shown below) if you want a successful access corresponding to one of those events to trigger the collection of the CIFS access log.</p> <p>Failed</p> <p>Select the check boxes for desired events (from the items shown below) if you want a failed access corresponding to one of those events to trigger the collection of the CIFS access log.</p> <p>Each of the following items is used to specify an event (or access):</p> <ul style="list-style-type: none"> • List folder contents • Read data • Create files or write data • Create folders • Delete items • Read permissions • Change permissions • Change ownership • Rename items • Connect to or disconnect from shares

FTP Service Management page

You can change the configuration definition of an FTP service.



Note:

- When the system administrator changes the configuration definitions of the FTP service, anonymous users are allowed to log on by using the FTP service. If an anonymous user logs on to the FTP service, the name `ftp` is used for the user name and group name.
- The service does not automatically restart even when the configuration definitions of the FTP service have been changed. If the configuration

definitions of the FTP service have been changed, restart the service by clicking **Restart** in the **List of Services** page.

- Even if the node is restarted after the configuration definitions of the FTP service are modified, the modified configuration definitions are not applied. Restart the service.
- If the system administrator changes the configuration definitions of the FTP service while a client is updating the file system, the client operation might not finish normally. The system administrator must contact users before changing the configuration definitions.
- When the `chmod` command is run on an FTP client for a file or directory for which an ACL is set, the ACL settings might become invalid. In this case, set the ACL again.

To display the **FTP Service Management** page, select **FTP** for **Service name** on the **List of Services** page, and then click the **Modify Configuration** button.

Table C-133 Items displayed on the FTP Service Management page

Item	Description
Specification method for a login directory	<p>Select the method of setting a directory to which the users can log on by using the FTP service.</p> <p>All mounted file systems can be used.</p> <p>Log on to the <code>/mnt</code> directory. This setting allows use of all file systems mounted on each node.</p> <p>Only the specified directory can be used.</p> <p>Log on to a specified file system or directory. This setting allows users to use only the specified file systems or directories.</p>
Login directory	<p>Specify the directory to which the users can log on by using the FTP service.</p> <p>If you select Only the specified directory can be used. in Specification method for a login directory, specify the path name of any file system or directory you want to use as the login directory. If you select All mounted file systems can be used., the system assumes <code>/mnt</code>.</p> <p>Use either of the methods below to specify the file system or directory to which the users can log on by using the FTP service. To display the List of Mounted File Systems page, click the Select button.</p> <ul style="list-style-type: none"> • On the List of Mounted File Systems page, select a file system. If you also want to specify a directory name, enter the directory name after the mount point displayed in the text box. • In the text box, directly enter the file system name or the directory name. <p>When you specify the login directory for the FTP service, make sure that you specify an absolute path name that begins with <code>/mnt/</code>. You cannot specify a path that includes a symbolic link.</p> <p>You can use any alphanumeric character, and the symbols below. Alphabetical characters are case sensitive. In addition, multi-byte</p>

Item	Description
	<p>characters can be specified. Note that a forward slash that is specified at the end is deleted.</p> <p>! # \$ % & ' () + , / ; = @ [] ^ ` { } ~</p> <p>When sharing a directory of the file system:</p> <p style="padding-left: 40px;"><i>/mnt/name-of-mounted-file-system/path-name</i></p> <p>Example: <i>/mnt/filesystem01/ftp1</i></p> <p>When sharing the whole of each file system:</p> <p style="padding-left: 40px;"><i>/mnt/name-of-mounted-file-system</i></p> <p>Example: <i>/mnt/filesystem02</i></p> <p>A mount point can be specified for a file system to which On (Read/Write) is selected for Content Sharing.</p> <p>You cannot specify a file system for which On (Read-Only) or Home directory is selected for Content Sharing.</p>
<p>Directory creation / change</p>	<p>Select whether to create a directory if the directory specified in Login directory does not exist. If the directory has been created, you can change the properties for the specified directory.</p> <p>If the directory specified in Login directory has already been created, and you want to use the directory without change, select Do not create / change. The system assumes Do not create / change if the specification of Login directory is <i>/mnt</i>.</p> <p>To create a directory or to change the attributes of an existing directory, select Create / Change. When you select Create / Change, select or enter the following items:</p> <p>Owner</p> <p style="padding-left: 40px;">Specify the user name or user ID of the owner.</p> <p>Group</p> <p style="padding-left: 40px;">Specify the group name or group ID of the owner group.</p> <p>Other</p> <p style="padding-left: 40px;">Set the directory access permissions for others.</p> <p>Permission mode[#]</p> <p style="padding-left: 40px;">Select the access permission for the directory owner, the owner's group, or other entity.</p> <p style="padding-left: 80px;">- Read / Write</p> <p style="padding-left: 40px;">Select this mode to grant both read and write permissions. The directory execution permission is granted.</p> <p style="padding-left: 80px;">- Read only</p> <p style="padding-left: 40px;">Select this mode to grant read permissions only. The directory execution permission is granted.</p> <p style="padding-left: 80px;">- None</p> <p style="padding-left: 40px;">Select this mode when neither the read and write permissions nor the directory execution permission is granted. This mode is available for Group and Other.</p> <p>Sticky bit</p> <p style="padding-left: 40px;">Select whether to set a sticky bit for the directory.</p> <p style="padding-left: 40px;">Setting a sticky bit allows only the owner of the directory to delete or rename the files or directories under that directory.</p>

Item	Description
	<p>- On Set a sticky bit.</p> <p>- Off Do not set a sticky bit.</p> <p>When you are not using user mapping, Specify the user and the group name no more than 16 characters. You can use any alphanumeric character, hyphen (-), period (.), and underscore (_).</p> <p>When you are using user mapping, specify a domain name with the user name or the group name as follows: <i>domain-name\user-name</i> <i>domain-name\group-name</i></p> <p>Specify a domain name using no more than 15 characters. The characters that can be used for the domain name are alphanumeric characters, exclamation mark (!), hash mark (#), percent sign (%), ampersand (&), left parenthesis ((), right parenthesis ()), hyphen (-), period (.), left angle bracket (<), caret (^), underscore (_), left curly bracket ({), right curly bracket (}), tilde (~), space and multi-byte characters that are encoded in UTF-8. When you are using user mapping, Specify the user name no more than 20 characters or the group name no more than 64 characters. The characters that can be used for the user name and the group name are alphanumeric characters, exclamation mark (!), hash mark (#), percent sign (%), ampersand (&), left parenthesis ((), right parenthesis ()), hyphen (-), period (.), left angle bracket (<), caret (^), underscore (_), left curly bracket ({), right curly bracket (}), tilde (~), space and multi-byte characters that are encoded in UTF-8.</p> <p>If you use the Active Directory authentication, specify the same domain name as specified in Domain name (NetBIOS).</p>
Allowed users	<p>Specify the users to be allowed to log on by using the FTP service.</p> <p>All users</p> <p>Allow all users to log on by using the FTP service. Note that the users registered by user mapping cannot log on by using the FTP service. To allow the users authenticated by Active Directory to log on, select Including Active Directory users.</p> <p>Selected users</p> <p>Allow the specified users to log on by using the FTP service. On the Select FTP Users page, select the users to be allowed to log on by using the FTP service. To display the Select FTP Users page, click the Set Up button. You can select a maximum of 2,000 users.</p> <p>The number of users currently allowed to log on is displayed to the right of this item name in the following format: Selected users(<i>number-of-users users</i>)</p>
Number of simultaneous connections	<p>Specify the number of uses who can concurrently log on by using the FTP service.</p> <p>Specify a number in the range from 10 to 500.</p>

Item	Description
Connection timeout wait time	Specify the timeout for an automatic logout in seconds. If no operation is performed within the timeout period after an FTP client has logged on to the directory, the FTP client is logged out automatically. Specify a number in the range from 30 to 43200.
Anonymous user settings	Select whether to allow anonymous users to log on by using the FTP service. Allow anonymous logins Select this to grant anonymous users permission to log on by using the FTP service. Anonymous users can use the FTP service with the ftp user (UID=97) and ftp group (GID=97) permissions. To grant anonymous users permission to upload, select Allow uploads . Do not allow anonymous logins Do not allow anonymous users to log on by using the FTP service.
# : Access permissions are set on a per-directory basis. Therefore, when the same directory is specified in Login directory for both the FTP and SFTP services, changing the access permission for either service will also change the access permission for the other service. In this case, you do not need to restart the other server to apply the change.	

Note the following for directories that must be logged on from the FTP service:

- A directory that an NFS client created by using a character encoding such as EUC or JIS cannot be specified as a directory that is logged on to from the FTP service.
- If a command is executed after logging on from the FTP service, the directory specified for **Login directory** becomes the root directory.

List of Mounted File Systems page

You can select which file systems users of the FTP or SFTP service can log on to.



Note: To allow access to a directory under a file system, on the **FTP Service Management** page or **SFTP Service Management** page, enter the directory following the mount point displayed for **Login directory**.

To display the **List of Mounted File Systems** page, on the **FTP Service Management** page or **SFTP Service Management** page, click the **Select** button for **Login directory**.

Table C-134 Items displayed on the List of Mounted File Systems page

Item	Description
File system	Displays the mounted file system.
Mount point	Displays the mount point for the file system.

Select FTP Users page

You can select the users that are permitted to log on to use the FTP service.

To display the **Select FTP Users** page, on the **FTP Service Management** page, click the **Set Up** button under **Allowed users**.

Table C-135 Items displayed on the Select FTP Users page

Item	Description
List of selectable users	<p>Select the users who will use the FTP service. To narrow down the users that are displayed, select the conditions from Condition, and then click the Display button.</p> <p>all Displays all user names.</p> <p>a to z, A to Z, or 0 to 9 Displays user names that begin with the selected alphanumeric character.</p> <p>other Displays user names that begin with a character other than an alphanumeric.</p> <p>The total number of filtered users is displayed to the right of Condition. A maximum of 1,000 users can be displayed at the same time in List of selectable users. If the number of users exceeds 1,000, you can use the following methods to specify the users that will be displayed:</p> <p>Range Displays the sequence number of the user who is displayed at the beginning of List of selectable users.</p> <ul style="list-style-type: none"> - Display button <p>Specify a value equal to or less than the total number of filtered users, and then click the Display button. This displays 1,000 users, beginning with the user whose sequence number you specified. If you then select a different filter from Condition and click the Display button, the value specified in Range is ignored and users are displayed beginning with the first user.</p> <ul style="list-style-type: none"> - Prev button <p>Clicking the Prev button displays in sequential order the users preceding the user displayed at the beginning of List of selectable users. If the user displayed at the beginning of List of selectable users is the first user, or if the total number of filtered users is 0, an error message appears when you click the Prev button.</p>

Item	Description
	<p>- Next button</p> <p>Clicking the Next button displays in sequential order the users following the user displayed at the end of List of selectable users. If the user displayed at the end of List of selectable users is the last user, or if the total number of filtered users is 0, an error message appears when you click the Next button.</p>
Selected users	<p>When you click the ▼ button, the users selected in List of selectable users are added to Selected users. Only users listed in Selected users will be set as users with the designated access permission.</p> <p>To delete a user from Selected users, select the user and click the ▲ button.</p>

NFS Service Management page

You can change the configuration definition of the NFS service.



Note:

- Even if the node is restarted after the configuration definitions of the NFS service are modified, the modified configuration definitions are not applied. Restart the service.
- When you stop the NFS service, ask the NFS client host's administrator to ensure that NFS shares are not accessed until the NFS service has started.
- If you change **Number of nfsd processes** in the configuration definitions of the NFS service, use the `nfsstatus` command to check the information about the current usage rate of the NFS daemon and the memory status, and then decide the appropriate number of NFS daemon processes. If the operation continues for a long time while the usage rate is high (90-100%), or if `Number of times that all threads were in use` is not 0, you need to increase the number of processes. If `Retry count of buffer acquisition` is not 0, the `nfsd` process has failed to secure the area for transfer and retries have occurred.
- Before changing the settings below, ask the NFS client host's administrator to unmount the file system from the NFS client side. If you change these settings before the NFS client host's administrator unmounts the file system, access to the file system from the NFS client will not be possible after the NFS service is restarted.
 - The value for **nfsd buffer size** is changed.
 - In **Protocol version, Security flavor, Domain name, and KDC server name(s)**, the settings for the items corresponding to the functions used by the NFS clients are canceled or changed.

After modifying the configuration definition, and restarting the NFS service, the system administrator must ask the NFS client host's administrator to remount the file system that was unmounted from the NFS client.

- If Kerberos authentication is used and the times of the HDI system and an NFS client host differ, authentication might fail for an NFS client accessing the HDI system. Use the NTP server to synchronize the times of the HDI system and the NFS client hosts.

To display the **NFS Service Management** page, select **NFS** for **Service name** on the **List of Services** page, and then click the **Modify Configuration** button.

Table C-136 Items displayed on the NFS Service Management page

Item	Description	See
NFS service settings	Specify the information for the NFS service.	Table C-137 Items displayed in NFS service settings on the NFS Service Management page on page C-169
NFS v4 setup	Specify the information required for using the NFSv4 protocol.	Table C-138 Items displayed in NFS v4 setup on the NFS Service Management page on page C-171

Table C-137 Items displayed in NFS service settings on the NFS Service Management page

Item	Description
Number of nfsd processes	Specify the maximum number of <code>nfsd</code> processes that can be started. Specify a number from 1 to 2048. During operation, the number of <code>nfsd</code> processes that are started is automatically adjusted according to the system status within the specified maximum value. However, if a value smaller than 64 is specified, the system applies 64 in actual operation. If 64 or a larger value is specified, the system rounds up the value to the nearest multiple of the number of CPUs when the service starts. For example, if 90 is specified when there are 16 CPUs, the system applies 96 in the actual operation.
nfsd buffer size	Enter the maximum buffer size for data transmission in KB units. Ask the NFS client host's administrator to unmount the file system from the NFS client before changing the maximum data size that can be transmitted. Specify a number from 8 to 1024. However, if NFS is mounted by using the UDP protocol, the maximum data size that can be transmitted is 56 KB, even if a value greater than 56 is specified.
Protocol version	Specify one or more of the NFS protocol versions to be used. v2 Select this to use NFSv2.

Item	Description
	<p>v3 Select this to use NFSv3.</p> <p>v4 Select this to use NFSv4.</p>
Port number allocation	<p>Specify how the port number is assigned to the NFS service.</p> <p>Dynamic Select this to dynamically assign a port number.</p> <p>Fixed Select this to assign a fixed port number.</p> <p>Privileged Select this to assign a privileged port number.</p>
Security flavor	<p>Specify one or more of the security flavors to be used.</p> <p>sys Select this to use the UNIX (AUTH_SYS) authentication.</p> <p>krb5 Select this to use the Kerberos authentication.</p> <p>krb5i Select this to use the data integrity function in addition to the Kerberos authentication.</p> <p>krb5p Select this to use the data integrity function and privacy function in addition to the Kerberos authentication.</p>
Domain name	<p>Specify the NFSv4 domain name or the name of the domain to which the KDC server belongs.</p> <p>Also, specify the domain to which the domain name is to be applied by selecting either of the following check boxes:</p> <p>Apply to an NFSv4 domain Select this to apply the name to an NFSv4 domain.</p> <p>Apply to a KDC server domain Select this to apply the name to a KDC server domain.</p> <p>If both the KDC server and the Active Directory domain controller are used as one server, the name specified here will also be used as the Active Directory domain controller name.</p> <p>If both the KDC server and the Active Directory domain controller are used as one server, and the specified name is different from the name of the Active Directory domain or domain controller used by the CIFS service, you need to restart the CIFS service.</p> <p>Any lower-case letters that are entered are treated as upper-case letters.</p>
KDC server name(s)	<p>Specify the KDC server name.</p> <p>Specify a server name beginning with an alphabetic character and consisting of alphanumeric characters, hyphens (-), and underscores (_), or specify an IP address.</p>

Item	Description
	<p>Up to five server names can be specified. When specifying multiple names, separate each with a comma (,). You can also specify the IP address.</p> <p>If both the KDC server and the Active Directory domain controller are used as one server, the name specified here will also be used as the Active Directory domain controller name.</p> <p>If both the KDC server and the Active Directory domain controller are used as one server, and the specified name is different from the name of the Active Directory domain or domain controller used by the CIFS service, you need to restart the CIFS service.</p>

Table C-138 Items displayed in NFS v4 setup on the NFS Service Management page

Item	Description
Anonymous user name	Specify a user name. This user name will be mapped to a user who belongs to a domain whose name is not set as an NFSv4 domain name for the NFS service, or who is not managed by the HDI system, when an access is made by the user. Specify a user name that has been registered in the HDI system, on the NIS server, or on the LDAP server for user authentication. The default is <code>nobody</code> (user ID: 65534).
Anonymous group name	Specify a group name. This group name will be mapped to a group that belongs to a domain whose name is not set as the NFSv4 domain name for the NFS service, or that is not managed by the HDI system, when an access is made by the group. Specify a group name that has been registered in the HDI system, on the NIS server, or on the LDAP server for user authentication. The default is <code>nogroup</code> (group ID: 65534).

SFTP Service Management page

You can change the configuration definition of an SFTP service.



Note:

- The service does not automatically restart even when the configuration definitions of the SFTP service have been changed. If the configuration definitions of the SFTP service have been changed, restart the service by clicking **Restart** in the **List of Services** page.
- Even if the node is restarted after the configuration definitions of the SFTP service are modified, the modified configuration definitions are not applied. Restart the service.
- If the system administrator changes the configuration definitions of the SFTP service while a client is updating the file system, the client operation might not finish normally. The system administrator must contact users before changing the configuration definitions.

- When the `chmod` command is run on an FTP client for a file or directory for which an ACL is set, the ACL settings might become invalid. In this case, set the ACL again.

To display the **SFTP Service Management** page, select **SFTP** for **Service name** on the **List of Services** page, and then click the **Modify Configuration** button.

Table C-139 Items displayed on the SFTP Service Management page

Item	Description
Specification method for a login directory	<p>Select the method of setting a directory to which the users can log on by using the SFTP service.</p> <p>All mounted file systems can be used.</p> <p>Log on to the <code>/mnt</code> directory. This setting allows use of all file systems mounted on each node.</p> <p>Only the specified directory can be used.</p> <p>Log on to a specified file system or directory. This setting allows users to use only the specified file systems or directories.</p>
Login directory	<p>Specify the directory to which the users can log on by using the SFTP service.</p> <p>If you select Only the specified directory can be used. in Specification method for a login directory, specify the path name of any file system or directory you want to use as the login directory. If you select All mounted file systems can be used., the system assumes <code>/mnt</code>.</p> <p>Use either of the methods below to specify the file system or directory to which the users can log on by using the SFTP service. To display the List of Mounted File Systems page^{#1}, click the Select button.</p> <ul style="list-style-type: none"> • On the List of Mounted File Systems page, select a file system. If you also want to specify a directory name, enter the directory name after the mount point displayed in the text box. • In the text box, directly enter the file system name or the directory name. <p>When you specify the login directory for the SFTP service, make sure that you specify an absolute path name that begins with <code>/mnt/</code>. You cannot specify a path that includes a symbolic link.</p> <p>You can use any alphanumeric character, and the symbols below. Alphabetical characters are case sensitive. In addition, multi-byte characters can be specified. Note that a forward slash that is specified at the end is deleted.</p> <p>! \$ % & ' () + , / ; @ [] ^ ` { } ~</p> <p>When sharing a directory of the file system:</p> <p><code>/mnt/name-of-mounted-file-system/path-name</code></p> <p>Example: <code>/mnt/filesystem01/sftp1</code></p> <p>When sharing the whole of each file system:</p> <p><code>/mnt/name-of-mounted-file-system</code></p>

Item	Description
	<p>Example: /mnt/filesystem02</p> <p>A mount point can be specified for a file system to which On (Read/Write) is selected for Content Sharing.</p> <p>You cannot specify a file system for which On (Read-Only) or Home directory is selected for Content Sharing.</p>
<p>Directory creation / change</p>	<p>Select whether to create a directory if the directory specified in Login directory does not exist. If the directory has been created, you can change the properties for the specified directory.</p> <p>If the directory specified in Login directory has already been created, and you want to use the directory without making any changes, select Do not create / change. The system assumes Do not create / change if the specification of Login directory is /mnt.</p> <p>To create a directory or to change the attributes of an existing directory, select Create / Change. When you select Create / Change, select or enter the following items:</p> <p>Owner</p> <p>Specify the user name or user ID of the owner.</p> <p>Group</p> <p>Specify the group name or group ID of the owner group.</p> <p>Other</p> <p>Set the directory access permissions for others.</p> <p>Permission mode^{#2}</p> <p>Select the access permission for the directory owner, the owner's group, or other entity.</p> <ul style="list-style-type: none"> - Read / Write <p>Select this mode to grant both read and write permissions. The directory execution permission is granted.</p> <ul style="list-style-type: none"> - Read only <p>Select this mode to grant read permissions only. The directory execution permission is granted.</p> <ul style="list-style-type: none"> - None <p>Select this mode when neither the read and write permissions nor the directory execution permission is granted. This mode is available for Group and Other.</p> <p>Sticky bit</p> <p>Select whether to set a sticky bit for the directory.</p> <p>Setting a sticky bit allows only the owner of the directory to delete or rename the files or directories under that directory.</p> <ul style="list-style-type: none"> - On <p>Set a sticky bit.</p> <ul style="list-style-type: none"> - Off <p>Do not set a sticky bit.</p> <p>When you are not using user mapping, Specify the user and the group name no more than 16 characters. You can use any</p>

Item	Description
	<p>alphanumeric character, hyphen (-), period (.), and underscore (_).</p> <p>When you are using user mapping, specify a domain name with the user name or the group name as follows:</p> <p><i>domain-name\user-name</i> <i>domain-name\group-name</i></p> <p>Specify a domain name using no more than 15 characters. The characters that can be used for the domain name are alphanumeric characters, exclamation mark (!), hash mark (#), percent sign (%), ampersand (&), left parenthesis ((), right parenthesis ()), hyphen (-), period (.), left angle bracket (<), caret (^), underscore (_), left curly bracket ({), right curly bracket (}), tilde (~), space and multi-byte characters that are encoded in UTF-8. When you are using user mapping, Specify the user name no more than 20 characters or the group name no more than 64 characters. The characters that can be used for the user name and the group name are alphanumeric characters, exclamation mark (!), hash mark (#), percent sign (%), ampersand (&), left parenthesis ((), right parenthesis ()), hyphen (-), period (.), left angle bracket (<), caret (^), underscore (_), left curly bracket ({), right curly bracket (}), tilde (~), space and multi-byte characters that are encoded in UTF-8.</p> <p>If you use the Active Directory authentication, specify the same domain name as specified in Domain name (NetBIOS).</p>
Allowed users	<p>Specify the users to be allowed to log on by using the SFTP service.</p> <p>All users</p> <p>Allow all users to log on by using the SFTP service. Note that the users registered by user mapping cannot log on by using the SFTP service. To allow the users authenticated by Active Directory to log on, select Including Active Directory users.</p> <p>Selected users</p> <p>Allow the specified users to log on by using the SFTP service. On the Select SFTP Users page, select the users to be allowed to log on by using the SFTP service. To display the Select SFTP Users page, click the Set Up button. You can select a maximum of 2,000 users.</p> <p>The number of users currently allowed to log on is displayed to the right of this item name in the following format:</p> <p>Selected users(number-of-users users)</p>
#1:	<p>For details about the List of Mounted File Systems page, see List of Mounted File Systems page on page C-166.</p>
#2:	<p>Access permissions are set on a per-directory basis. Therefore, when the same directory is specified in Login directory for both the FTP and SFTP services, changing the access permission for either service will also change the access permission for the other service. In this case, you do not need to restart the other server to apply the change.</p>

Note the following points when you set a directory that must be logged on to from the SFTP service:

- A directory that an NFS client created by using a character encoding such as EUC or JIS cannot be specified as a directory that is logged on to from the SFTP service.
- For the SFTP service, directories above the directory specified for **Login directory** cannot be accessed.

Select SFTP Users page

You can select the users that are permitted to log on to use the SFTP service.

To display the **Select SFTP Users** page, on the **SFTP Service Management** page, click the **Set Up** button under **Allowed users**.

Table C-140 Items displayed on the Select SFTP Users page

Item	Description
List of selectable users	<p>Select the users who will use the SFTP service. To narrow down the users that are displayed, select conditions from Condition, and then click the Display button.</p> <p>all</p> <p>Displays all user names.</p> <p>a to z, A to Z, or 0 to 9</p> <p>Displays user names that begin with the selected alphanumeric character.</p> <p>other</p> <p>Displays user names that begin with a character other than an alphanumeric.</p> <p>The total number of filtered users is displayed to the right of Condition. A maximum of 1,000 users can be displayed at the same time in List of selectable users. If the number of users exceeds 1,000, you can use the following methods to specify the users that will be displayed:</p> <p>Range</p> <p>Displays the sequence number of the user who is displayed at the beginning of List of selectable users.</p> <ul style="list-style-type: none"> - Display button <p>Specify a value equal to or less than the total number of filtered users, and then click the Display button. This displays 1,000 users, beginning with the user whose sequence number you specified. If you then select a different filter from Condition and click the Display button, the value specified in Range is ignored and users are displayed beginning with the first user.</p> <ul style="list-style-type: none"> - Prev button <p>Clicking the Prev button displays in sequential order the users preceding the user displayed at the beginning of List of selectable users. If the user displayed at the beginning of List of selectable users is the first user, or if the total number of filtered users is 0, an error message appears when you click the Prev button.</p>

Item	Description
	<p>- Next button</p> <p>Clicking the Next button displays in sequential order the users following the user displayed at the end of List of selectable users. If the user displayed at the end of List of selectable users is the last user, or if the total number of filtered users is 0, an error message appears when you click the Next button.</p>
Selected users	<p>When you click the ▼ button, the users selected in List of selectable users are added to Selected users. Only users listed in Selected users will be set as users with the designated access permission.</p> <p>To delete a user from Selected users, select the user and click the ▲ button.</p>

Public Key List page

You can register and delete public keys.

To display the **Public Key List** page, select **SSH** for **Service name** on the **List of Services** page, and then click the **Modify Configuration** button.

Table C-141 Items displayed on the Public Key List page

Item	Description
SSH protocol version	Displays the version of the SSH protocol.
Comment	Displays any comments about the public key.
Delete button	Deletes the public key.
Add button	Add the public key. The Add Public Key page is displayed (Add Public Key page on page C-176).

Add Public Key page

A system administrator can add a public key in the **Add Public Key** page.



Note:

- Use a key creation tool to create the keys (private key and public key) that are used in the SSH authentication. For details about how to install the relevant software and create those keys, see the documentation provided with the software.
- Public keys are registered for the SSH account `nasroot`.
- The number of public keys must not be more than 128.

To display the **Add Public Key** page, click the **Add** button on the **Public Key List** page.

Table C-142 Items displayed on the Add Public Key page

Item	Description
SSH protocol version	Displays the version of the SSH protocol.
Public key file	Specify the path to the public key file. To select a file name through browsing, click the Browse button.
Comment	Enter a comment about the public key. Enter a maximum of 32 characters. You can use alphanumeric characters and hyphens (-). You can also specify spaces, but not at the beginning or end of the character string.

CIFS Service Maintenance page

You can view the configuration definition for a CIFS service, delete cached user mapping information, and rejoin the Active Directory domain.

To display the **CIFS Service Maintenance** page, click **CIFS** in **Service name** on the **List of Services** page, and then click the **Service Maintenance** button.

Table C-143 Items displayed on the CIFS Service Maintenance page

Item	Description
CIFS service information area	Displays information about the operating status of the CIFS service. For details about the items displayed, see Table C-144 Items displayed on the CIFS service information area of the CIFS Service Maintenance page on page C-178 .
CIFS default information area	Displays information about accesses from the clients. For details about the items displayed, see Table C-145 Items displayed on the CIFS default information area of the CIFS Service Maintenance page on page C-181 .
User mapping information area	Displays information about user mapping. The displayed information differs depending on which user mapping method is used. For details about the items displayed, see Table C-146 Items displayed in the User mapping information area of the CIFS Service Maintenance page (when user mapping uses RIDs) on page C-184 , Table C-147 Items displayed in the User mapping information area of the CIFS Service Maintenance page (when user mapping uses LDAP) on page C-184 , or Table C-148 Items displayed in the User mapping information area of the CIFS Service Maintenance page (when user mapping uses the Active Directory schema) on page C-186 . If user mapping is not used, Not used is displayed for User mapping usage type .
Clear User Map Cache File button	Deletes cached user mapping information.

Item	Description
Rejoin Active Directory Domain button	Rejoins the Active Directory domain.
Redefine Active Directory Domain button	Redefine the domain with which a trust relationship is to be established.

Table C-144 Items displayed on the CIFS service information area of the CIFS Service Maintenance page

Item	Description
Service status	<p>Displays the status of the CIFS service.</p> <p>Running Displayed when the CIFS service is running normally.</p> <p>Down Displayed when the service is running in an incomplete state.</p> <p>Offline Displayed when the resource group is stopped.</p> <p>Stopped Displayed when the CIFS service is stopped.</p>
Automatic startup of service	<p>Displays whether the CIFS service automatically starts when the OS is started or restarted.</p> <p>On Displayed when the CIFS service automatically starts.</p> <p>Off Displayed when the CIFS service does not automatically start.</p>
Service information	<p>The information about the CIFS service operating status is displayed.</p> <p>The configuration has been modified. Restart the service. Rebooting the OS will not apply the changes. Displayed when the CIFS service is not stopped after the service configuration is changed. Restart the service. Rebooting the OS will not apply the changes.</p> <p>The configuration has been modified. Start the service. Rebooting the OS will not apply the changes. Displayed when the CIFS service is stopped after the service configuration is changed. Start the service. Rebooting the OS will not apply the changes.</p> <p>The service is incomplete. Restart the service. Displayed when the service is running in an incomplete state. If this information appears, restart the service.</p>
SMB protocol	The SMB protocol to be used for gaining access from the CIFS client is displayed.

Item	Description
	<p>SMB 1.0 Displayed when SMB 1.0 is being used.</p> <p>SMB 2.0 Displayed when SMB 2.0 is being used. SMB 1.0 can also be used.</p> <p>SMB 2.1 Displayed when SMB 2.1 is being used. SMB 1.0 and SMB 2.0 can also be used.</p> <p>SMB 3.0 Displayed when SMB 3.0 is being used. SMB 1.0, SMB 2.0, and SMB 2.1 can also be used.</p>
Server comment	Displays a comment on the server name displayed on the CIFS client.
Authentication mode	<p>Displays information about the authentication mode and authentication server.</p> <p>Local authentication</p> <p>Displayed when local authentication is being used.</p> <p>Workgroup name</p> <p>Displays the work group name.</p> <p>NT domain authentication</p> <p>Displayed when NT domain authentication is being used.</p> <p>Domain name</p> <p>Displays the domain name.</p> <p>PDC server name</p> <p>Displays the server name of the primary domain controller.</p> <p>BDC server name</p> <p>Displays the server name of the backup domain controller.</p> <p>Domain administrator name</p> <p>Displays the user name of the domain administrator.</p> <p>Active Directory authentication</p> <p>Displayed when Active Directory authentication is being used.</p> <p>Domain name</p> <p>Displays the domain name of the Active Directory domain.</p> <p>Domain name (NetBIOS)</p> <p>Displays the NetBIOS name of the Active Directory domain.</p> <p>DC server name(s)</p> <p>Displays the server name of the Active Directory domain controller.</p> <p>Domain user name</p>

Item	Description
	Displays the name of the user for the Active Directory domain controller.
DC server connection status	Displays the connection status of the user authentication server. When there is at least one domain controller server to which you can connect, <code>Connectable</code> is displayed.
Host access restrictions	<p>When only certain CIFS clients are allowed access to the CIFS share, the host names or IP addresses of those CIFS clients, or the network addresses of the networks to which the clients belong, are displayed after <code>Allow</code>. Alternatively, when certain CIFS clients are to be denied access to the CIFS share, the host names or IP addresses of those CIFS clients, or the network addresses of the networks to which the clients belong, are displayed after <code>Deny</code>.</p> <p>When all CIFS clients are allowed access to the CIFS share, nothing is displayed.</p>
Client time-out	Displays the client timeout value (in minutes). If 0 is displayed, automatic disconnection due to a timeout is not performed.
Mapping to guest account	<p>Displays what kind of users will be treated as guests.</p> <p><code>Unregistered users</code></p> <p>Displayed when users who have not been registered in the system will be treated as guests.#</p> <p><code>Unregistered users or invalid passwords</code></p> <p>Displayed when users who have not been registered in the system or who have been registered in the system but have an invalid password will be treated as guests.#</p> <p><code>Never</code></p> <p>Displayed when guest access to the CIFS shares is not permitted.</p>
NetBIOS over TCP/IP	<p>Displays whether to accept access, from CIFS clients, that uses NetBIOS over TCP/IP.</p> <p><code>Use</code></p> <p>Displayed when the CIFS service accepts access, from CIFS clients, that uses NetBIOS over TCP/IP.</p> <p><code>Do not use</code></p> <p>Displayed when the CIFS service does not accept access, from CIFS clients, that uses NetBIOS over TCP/IP.</p>
CIFS access log	<p>Displays whether the CIFS access log is collected.</p> <p><code>Use</code></p> <p>Displayed when the CIFS access log is collected.</p> <p><code>Use (If the CIFS access log file exceeds the max size, do not collect log data.)</code></p> <p>Displayed if the log file cannot be moved (when the move destination is not specified, or when the capacity of the file system to which the log file is to be moved has reached the maximum limit), and if you want to stop</p>

Item	Description
	collecting the CIFS access log at the time when the capacity of the log file reaches the maximum limit. Do not use Displayed when the CIFS access log is not collected.
Automatic reloading of CIFS share settings	Displays whether the CIFS share settings are automatically reloaded when they are changed. Perform Displayed when the CIFS share settings are automatically reloaded. Do not perform Displayed when the CIFS share settings are not automatically reloaded.
Max. number of CIFS clients accessible simultaneously	Displays the maximum value of CIFS clients that can access a node.
CIFS administrator name(s)	When one or more users or groups have been set as CIFS administrators, this item displays their user names or group names.
Current number of CIFS login clients	Displays the number of CIFS clients that are currently logged on.
<p>#: The users to be treated as guests differ depending on the authentication mode that is currently used (the mode displayed in Authentication mode):</p> <ul style="list-style-type: none"> • When Local authentication is being used Users who are not registered by using local authentication are treated as guests. • When NT domain authentication is being used Users who are not registered in the domain controller in the domain are treated as guests. • When Active Directory authentication is being used Users who are not registered in the Active Directory domain controller are treated as guests. 	

Table C-145 Items displayed on the CIFS default information area of the CIFS Service Maintenance page

Item	Description
Guest account access	Displays whether guest account users access is allowed for the CIFS shares. Allow Displayed when guest account users access is allowed. Disallow Displayed when guest account users access is disallowed.
Disk synchronization policy	Displays operational settings for write requests from CIFS clients to CIFS shares. At write and close

Item	Description
	<p>Displayed when writing is performed synchronously with a write request or a close request.</p> <p>At close</p> <p>Displayed when writing is performed synchronously with a close request.</p> <p>Routine disk flush only</p> <p>Displayed when writing is performed at a fixed interval, regardless of when write requests and close requests are made.</p>
Windows® client access policy	<p>Displays the method for processing accesses from Windows clients.</p> <p>Parallel</p> <p>Displayed when accesses are processed in parallel.</p> <p>Serial</p> <p>Displayed when accesses are processed serially.</p>
CIFS client cache	<p>Displays whether the updated data in the CIFS share file is to be cached on the client.</p> <p>Use</p> <p>Displayed when the updated data in the CIFS share file is to be cached on the client.</p> <p>Do not use</p> <p>Displayed when the updated data in the CIFS share file is not to be cached on the client.</p>
Read-only client cache for access conflicts	<p>Displays whether to use a read-only client cache when multiple CIFS clients simultaneously attempt to access a file.</p> <p>Use</p> <p>Displayed when a read-only client cache is used.</p> <p>Do not use</p> <p>Displayed when a read-only client cache is not used.</p>
Volume Shadow Copy Service	<p>Displays whether to use Volume Shadow Copy Service to make past versions of files that have been migrated to an HCP system available to CIFS clients.</p> <p>Use</p> <p>Displayed when Volume Shadow Copy Service is used.</p> <p>Do not use</p> <p>Displayed when Volume Shadow Copy Service is not used.</p>
Access Based Enumeration	<p>Displays whether to use access-based enumeration.</p> <p>Use</p> <p>Displayed when access-based enumeration is used.</p> <p>Do not use</p> <p>Displayed when access-based enumeration is not used.</p>
File timestamp changeable users	<p>Displays the users for whom you allow updating of CIFS share file timestamps.</p>

Item	Description
	<p>Write permitted users</p> <p>Displayed when you permit updating of the CIFS share file timestamp for all users who are permitted to write to this file.</p> <p>Owner only</p> <p>Displayed when you restrict timestamp updating to the file owner.</p> <p>Note that this setting is invalid in an advanced ACL file system. Only a user who has write permission can update timestamps.</p>
<p>Events logged to the CIFS access log</p>	<p>Displays the events that trigger the collection of the CIFS access log.</p> <p>Successful</p> <p>Selected the check boxes for desired events (from the items shown below) when a successful access corresponding to one of these items triggers the collection of the CIFS access log.</p> <p>Failed</p> <p>Selected the check boxes for desired events (from the items shown below) when a failed access corresponding to one of these items triggers the collection of the CIFS access log.</p> <p>Each of the following items is used to specify an event (or access):</p> <ul style="list-style-type: none"> • List folder contents • Read data • Create files or write data • Create folders • Delete items • Read permissions • Change permissions • Change ownership • Rename items • Connect to or disconnect from shares
<p>SMB encryption</p>	<p>Displays whether the communication with the CIFS client is to be encrypted when you use SMB 3.0.</p> <p>Auto</p> <p>Displayed when the communication with the client is to be encrypted only when the client supports encryption.</p> <p>Mandatory</p> <p>Displayed when the communication with the client is always to be encrypted.</p> <p>Disable</p> <p>Displayed when the communication with the client is not to be encrypted.</p>

Table C-146 Items displayed in the User mapping information area of the CIFS Service Maintenance page (when user mapping uses RIDs)

Item	Description
User mapping usage type	Displays the type of user mapping being used. If user mapping uses RIDs, <code>RID</code> is displayed.
Range of UIDs and GIDs	Displays the range of user IDs and group IDs mapped by using RIDs.
Settings for each domain	Displays the range of user IDs and group IDs set for each domain. When two or more ranges have been set, they are displayed in ascending order of the minimum value for the range of user IDs and group IDs.

Table C-147 Items displayed in the User mapping information area of the CIFS Service Maintenance page (when user mapping uses LDAP)

Item	Description
User mapping usage type	Displays the type of user mapping being used. If user mapping uses LDAP, <code>LDAP</code> is displayed.
LDAP server name	Displays the host name or IP address of the LDAP server.
LDAP server port number	Displays the port number of the LDAP server.
LDAP server root DN	Displays the identification name of the LDAP server root in DN format.
LDAP user map DN	Displays the identification name for which you added the user mapping account of the LDAP server in DN format.
LDAP administrator DN	Displays the identification name of the LDAP server administrator in DN format.
Allocation method	Displays the method for allocating user IDs and group IDs. <code>Automatic</code> Displayed when IDs are allocated automatically. <code>Manual</code> Displayed when IDs are allocated manually.
Range of UIDs	Displays the range of user IDs mapped by using LDAP. This information is displayed only when the setting for automatically assigning user IDs and group IDs is specified.
Largest currently used UID	Displays the largest user ID within the range of user IDs that have already been assigned in the HDI system.

Item	Description
	<p>This information is displayed only when the setting for automatically assigning user IDs and group IDs is specified.</p> <p>Depending on the status of user mapping usage, the following information might be displayed:</p> <p>Not used, or less than the minimum UID used.</p> <p>Displayed when no user IDs have been assigned, or the smallest assigned user ID is smaller than the minimum value set in Range of UIDs.</p> <p>Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.</p> <p>Displayed when the largest ID could not be acquired from the LDAP server for user mapping. Check the user mapping settings and the operating status of the LDAP server.</p>
Range of GIDs	<p>Displays the range of group IDs mapped by using LDAP.</p> <p>This information is displayed only when the setting for automatically assigning user IDs and group IDs is specified.</p>
Largest currently used GID	<p>Displays the largest group ID within the range of group IDs that have already been assigned in the HDI system.</p> <p>This item is displayed only when the setting for automatically assigning user IDs and group IDs is specified.</p> <p>Depending on the status of user mapping usage, the following information might be displayed:</p> <p>Not used, or less than the minimum GID used.</p> <p>Displayed when no group IDs have been assigned, or the smallest assigned group ID is smaller than the minimum value set in Range of GIDs.</p> <p>Cannot be got from LDAP server. Check the LDAP server settings and CIFS service configuration in service.</p> <p>Displayed when the largest ID could not be acquired from the LDAP server for user mapping. Check the user mapping settings and the operating status of the LDAP server.</p>

Table C-148 Items displayed in the User mapping information area of the CIFS Service Maintenance page (when user mapping uses the Active Directory schema)

Item	Description
User mapping usage type	Displays the type of user mapping being used. If user mapping uses an Active Directory schema, <code>Active Directory schema</code> is displayed.
Name service switch	Displays the name service switch being used. <code>Microsoft® Services for Unix</code> Displayed when Microsoft services for Unix is used. <code>Using LDAP as a network information service (RFC2307)</code> Displayed when the RFC2307 schema is used.
Joined domain name	Displays the name of the domain that the node is joined to.
Trusted domain name	Displays the names of the domains that have a trust relationship with the domain that the node is joined to. - is displayed if there are no such domains.

Virus Scan Server Configuration dialog box

In the **Virus Scan Server Configuration** dialog box, a system administrator can manage the real-time virus scanning functionality.

To display the **Virus Scan Server Configuration** dialog box, click **Virus Scan Server Configuration** in the **Settings** area of the *host-name* window.

List of Scanner Servers page

You can view information about real-time scanning set for the HDI system.

To display the **List of Scanner Servers** page, click **Virus Scan Server Configuration** in the **Settings** area of the *host-name* window.

Table C-149 Items displayed on the in the List of Scanner Servers page

Item	Description
Scanning software	Displays the name of the scan software that is used. If a scan software is not set, - is displayed.
Real-time scanning status	Displays the real-time scanning status. <code>Running</code> Displayed when real-time scanning is enabled. <code>Stopped</code> Displayed when real-time scanning is disabled.

Item	Description
Server address	Displays either the IP address, domain name, or host name of the scan server. Displays the content of the Server address specified in the Add Scanner Server page.
Server status	<p>Displays the status of the scan server.</p> <p>-</p> <p>Displayed when real-time scanning is disabled.</p> <p>Normal</p> <p>Displayed when the scan server is functioning normally.</p> <p>Blocked (Server not found)</p> <p>Displayed when the scan server cannot be found. Make sure that the IP address, domain name, or host name of the scan server is correct.</p> <p>Blocked (Access is impossible)</p> <p>Displayed when the port numbers set in the HDI system and the scan server are different, the real-time virus scan service is not available, or the virus scan software specified in the HDI system differs from the software on the scan server. Make sure that the IP address, domain name, or host name of the scan server, and the port number of the scan server, are correct. Also make sure that ICAP is selected as the communication protocol for the scan server, and that the scan software is correctly set in the HDI system.</p> <p>Blocked (Time-out)</p> <p>The scan server timed out. Make sure that no network failure has occurred.</p> <p>Blocked (Version conflict)</p> <p>The protocol versions for the HDI system and the scan server are incompatible. Acquire all the log data, and then inform maintenance personnel.</p> <p>Blocked (License expired)</p> <p>The license of the scan software installed on the scan server is invalid. Make sure that the scanning software license has been set up.#</p> <p>Blocked (Scanner server error)</p> <p>A failure occurred in the scan server. Recover the scan server from the failure.</p> <p>Blocked (Under registration)</p> <p>Displayed while the information about the registered scan server is being applied to an HDI system. Wait for several minutes, and then click Refresh to update the displayed information.</p> <p>Blocked (Invalid protocol)</p> <p>Displayed when the communication protocol is different from the one used by Hitachi Server Protect Agent that is installed on the scan server. Check the version of the installed Hitachi Server Protect Agent, and then install the correct version.</p> <p>Blocked (Scanning software is not installed)</p>

Item	Description
	<p>Displayed when scan software is not installed on the scan server. Install scan software.</p> <p>Blocked (Scanning software service has stopped)</p> <p>The service of the scan software on the scan server stopped. Start the service.</p> <p>Blocked (Access user info. is not registered)</p> <p>Displayed when the information of the user for accessing CIFS shares is not registered on the scan server. Register the information.</p> <p>Blocked (Access user info. is invalid)</p> <p>Displayed when the information of the user for accessing CIFS shares registered on the scan server is incorrect. Correct the information.</p> <p>Deleting</p> <p>Displayed when operation for deleting the scan server is performed, but some CIFS clients are using the scan server. The scan server will be deleted when the CIFS clients finish using the scan server.</p> <p>Error (System failure)</p> <p>Displayed when a failure occurred in the HDI system, or an attempt to update the status failed. Wait for the time specified for Server monitoring interval on the Scan Conditions page to pass, and then check the status again.</p> <p>If the status still cannot be updated, acquire all the log data, and then inform maintenance personnel.</p>
Software version	<p>Displays the version of the scan software that is installed on the scan server.</p> <p>If the scan software being used is Trend Micro ServerProtect, or if this information cannot be obtained, a hyphen (-) is displayed.</p>
Virus definition version	<p>Displays the version of the virus definition file used on the scan server.</p> <p>If the scan software being used is Trend Micro ServerProtect, or if this information cannot be obtained, a hyphen (-) is displayed.</p>
Edit Server button	<p>Edits the information for a scan server. Select the radio button for the scan server for which you want to change the registered information, and then click the Edit Server button. The Edit Scanner Server page is displayed (Edit Scanner Server page on page C-189).</p>
Delete Server button	<p>Deletes a scan server.</p> <p>Select the server you want to delete in the options, and then click Delete Server.</p>
Add Server button	<p>Registers a scan server. The Add Scanner Server page is displayed (Add Scanner Server page on page C-189).</p>
Scan Conditions button	<p>Sets the conditions for real-time scanning to be requested to a scan server. The Scan Conditions page is displayed (Scan Conditions page on page C-190).</p>

Item	Description
Scanning Software button	Sets the scan software to use. The Scanning software page is displayed (Scanning software page on page C-196).
Start button or Stop button	<p>Enables or disables real-time scanning. Click the Start button to enable real-time scanning. Click the Stop button to disable real-time scanning.</p> <p>Before enabling or disabling real-time virus scanning, note the following:</p> <ul style="list-style-type: none"> • After you enable or disable the real-time scanning, restart the CIFS service. • If you disable real-time virus scanning during scan processing, the scan processing might end with an error.
#: If you are using Trend Micro InterScan Web Security Virtual Appliance, even if the license is invalid, the message <code>Blocked (License expired)</code> will not be displayed. Check whether your license is valid on the InterScan Web Security Virtual Appliance server.	

Edit Scanner Server page

You can change the registered information for a scan server.

To display the **Edit Scanner Server** page, from the **List of Scanner Servers** page in the **Virus Scan Server Configuration** dialog box, select the radio button of the scan server for which you want to change the registered information, and then click the **Edit Server** button.

Table C-150 Items displayed on the Edit Scanner Server page

Item	Description
Server address	Specify the IP address, domain name, or host name of the scan server.
Port number	Specify a port number of the scan server.

Add Scanner Server page

A system administrator can register a scan server in **Add Scanner Server** page.

To display the **Add Scanner Server** page, click the **Add Server** button from the **List of Scanner Servers** page in the **Virus Scan Server Configuration** dialog box.

Table C-151 Items displayed on the Add Scanner Server page

Item	Description
Server address	Specify the IP address, domain name, or host name of the scan server.
Port number	Specify a port number of the scan server, from 1024 to 65535.

Item	Description
Add button	Registers the scan server.

Scan Conditions page

A system administrator can set scan conditions in **Scan Conditions** page.



Note:

- The scan server receives a scan request from a node, and then performs real-time scanning based on the scan server settings. For example, if the extension of a file in the scan request from the node is specified not to be scanned for the scan server, real-time scanning is not performed. For details about the scan server environment settings and scanning software settings, see the *Installation and Configuration Guide*.
- For details about how to remove files and paths in a CIFS share as scanning targets, see the *CLI Administrator's Guide*.

To display the **Scan Conditions** page, click the **Scan Conditions** button from the **List of Scanner Servers** page in the **Virus Scan Server Configuration** dialog box.

Table C-152 Items displayed on the Scan Conditions page

Item	Description
Scan timing ^{#1}	<p>Select the timing of scans in the options.</p> <p>Read and write Executes a scan when the CIFS client has read or written files.</p> <p>Read only Executes a scan when the CIFS client has read files.</p> <p>Write only Executes a scan when the CIFS client has written files.</p>
Extension for scanning	<p>Select the files to be scanned in the options. When Symantec scan software, McAfee scan software, or Trend Micro InterScan Web Security Virtual Appliance is used, this item can be displayed and set.</p> <p>Scan all files regardless of extension Scans all the files for viruses.</p> <p>Scan all files except these extensions Executes a scan on files other than those whose extensions were specified in the Extensions list box.</p> <p>Scan files with these extensions</p>

Item		Description
		Executes a scan on files whose extensions were specified in the Extensions list box.
Extensions	List box	<p>Specify the extensions to be used when you selected either the Scan all files except these extensions or Scan files with these extensions options in the Extension for scanning field, using no more than 16 characters. When Symantec scan software, McAfee scan software, or Trend Micro InterScan Web Security Virtual Appliance is used, this item can be displayed and set.</p> <p>Specify a maximum of 255 characters for each compatible option.</p> <p>When the Scan all files except these extensions option is selected, the default setting will appear in the list box as follows:</p> <pre>.aif, .aifc, .aiff, .asc, .au, .avi, .bmp, .eps, .gif, .ief, .jpe, .jpeg, .jpg, .kar, .latex, .log, .mid, .midi, .mov, .movie, .mp2, .mp3, .mpe, .mpeg, .mpg, .mpga, .pbm, .pcx, .pdf, .pgm, .png, .pnm, .ppm, .ps, .qt, .ra, .ram, .rgb, .rm, .rof, .snd, .swf, .tex, .texi, .texinfo, .tif, .tiff, .tsv, .wav, .xbm, .xpm, and .xwd</pre> <p>When the Scan files with these extensions option is selected, there is no default settings in the list box.</p> <p>The settings corresponding to the selected option will be saved by the system.</p> <p>Enter an extension and click Add to add an extension in the list box.</p> <p>To delete an extension from the list box, select it and click Delete.</p>
	Add button	Adds an extension to the list box. Enter the extension in the list box, and then click this button. Only the information that has been added to the list box will be set.
	Delete button	Deletes an extension from the list box. Select the extension to be deleted, and then click this button.
	Default Extensions button	Discards the settings saved in the system, and returns the extension settings to the defaults.
	Include files with no extension check box	Specifies that files without extensions will be scanned. It is also possible to specify that files without extensions will not be scanned.
Maximum size for scanning		Select whether or not to specify an upper limit for the size of files to be scanned in the options. When Symantec scan software, McAfee scan software, or Trend Micro

Item	Description
	<p>InterScan Web Security Virtual Appliance is used, this item can be displayed and set.</p> <p>Specify</p> <p>Select this option to perform a scan on all files whose size is the same as or smaller than the size specified in Maximum file size.</p> <p>Select this option to perform a scan on all files whose size is the same as or smaller than the size specified in Maximum file size.</p> <p>In the Maximum file size field, specify the upper size limit (in megabytes) of the file to be scanned within the range from 1 to 9,999 MB.</p> <p>To permit access for files larger than the limit specified in Maximum file size, select the Permit access to files that have exceeded the maximum size check box. This means that even if the file size exceeds that specified in Maximum file size, it will be stored within the storage system.</p> <p>Do not specify</p> <p>Select this option when not limiting the size of the file to be scanned.</p> <p>For Symantec Corporation virus scan software, an attempt to scan a file whose size is 2 GB or greater causes an error. Specify the file size in Maximum size for scanning as follows:</p> <ul style="list-style-type: none"> • Select the Specify radio button. • Specify a value equal to or less than 2,047 in the Maximum file size text box. • Select the Permit access to files that have exceeded the maximum size check box. <p>If a scan condition other than shown above is set, the CIFS clients can no longer access files whose size is 2 GB or greater. In addition, the scan server is blocked when the scanning fails.</p>
<p>Method of dealing with infected file^{#2}</p>	<p>Select the method of dealing with infected files from the drop down menu if an infected file that cannot be repaired is detected in the scan server. When Symantec scan software, McAfee scan software, or Trend Micro InterScan Web Security Virtual Appliance is used, this item can be displayed and set.</p> <p>Delete the file</p> <p>Select this option to delete infected files.</p> <p>Deny access</p>

Item	Description
	<p>Select this option to deny access from the client to infected files.</p> <p>Allow access</p> <p>Select this option to allow access from the client to infected files.</p> <p>Depending on the method of dealing with infected files, the operation result for the client accessing the infected file differs.</p> <p>When the client creates the target file, the operation result is as follows: An error is not reported to the operation result.</p> <p>When selecting Delete the file</p> <p>The target file is deleted and therefore cannot be created newly.</p> <p>When selecting Deny access</p> <p>The target file is deleted and therefore cannot be created newly.</p> <p>When selecting Allow access</p> <p>The target file can be created newly.</p> <p>When the client views the target file, the operation result is as follows:</p> <p>When selecting Delete the file</p> <p>The target file is deleted and therefore cannot be viewed.</p> <p>When selecting Deny access</p> <p>The target file access is denied. The target file cannot be viewed.</p> <p>When selecting Allow access</p> <p>The target file can be viewed.</p> <p>When the client updates the target file, the operation result is as follows: An error is not reported to the operation result.</p> <p>When selecting Delete the file</p> <p>The target file is deleted and therefore cannot be updated.</p> <p>When selecting Deny access</p> <p>The target file status returns to the status before the update and therefore the target file cannot be updated.</p> <p>When selecting Allow access</p> <p>The target file can be updated.</p>
<p>Notification when infection is detected</p>	<p>When SNMP or email error notifications are used, from the radio buttons, select whether you want to receive notifications regarding the results of infected files via the KAQV10022-E message.</p> <p>For details about messages other than KAQV10022-E that are output, and about</p>

Item	Description
	<p>message IDs that are sent via notifications by SNMP traps or email notifications (including message IDs that need to be set by the <code>avaconfedit</code> command in order to be sent by SNMP traps or email notifications), see the manual <i>Error Codes</i>.</p> <p>When Symantec scan software, McAfee scan software, or Trend Micro InterScan Web Security Virtual Appliance is used, this item can be displayed and set.</p> <p>Notify</p> <p>Select this option to send the KAQV10022-E message when infected files are detected.</p> <p>Do not notify</p> <p>Select this option if you do not want to be notified when infected files are detected.</p>
Connection time-out period	<p>Specify the interval from the time the connection request is sent from the HDI to the scan server until timeout, within the range from 1 to 600 seconds.</p> <p>Scan servers that do not respond during the timeout will be blocked, and the scan will be requested from another scan server.</p>
Scanning time-out period	<p>Specify the interval from the time a scan request is sent from the HDI to the scan server until timeout, within the range from 1 to 1,800 seconds.</p> <p>If there is no response within the specified amount of time, the response method selected in the Procedure if scanning fails field will be followed.</p>
Stub file scanning time-out period	<p>Specify the interval from the time a stub file scan request is sent from the HDI system to the scan server until the scanning times out. Specify a value in the range from 1 to 1,800 seconds.</p> <p>If there is no response within the specified amount of time, the response method selected in the Procedure if scanning fails field will be followed.</p>
Retry other server count	<p>Specify the number of times to switch the scan server in the event of a timeout or error during processing for connecting to the scan server.</p> <p>Specify a value from 0 to 32 that is no larger than the number of scan servers registered in the HDI.</p> <p>Specifying 0 will cause scans to fail when a timeout or error occurs during processing for connecting to the scan server.</p>

Item	Description
<p>Procedure if scanning fails</p>	<p>Select the response method you want to use, in the options, in the event that the scan fails.</p> <p>Allow access</p> <p>Specify this to permit access to files that could not be scanned for viruses.</p> <p>Deny access</p> <p>Specify this to refuse access to files that could not be scanned for viruses.</p> <p>Select the check box Permit read files if all scan server connections are closed and scan conditions are not satisfied if all scan server connections are closed and you only want to give a client permission to read files that are not excluded from being scanned (that is, folders and files with a folder or file size of zero and files that do not meet a scan condition).</p> <p>If this check box is not selected, any client access to read a file is denied.</p> <p>Even if all scan server connections are closed, files that are excluded from being scanned can also be stored in the storage system.</p> <p>Depending on the method of dealing with files that could not be scanned, the operation result for the client accessing such a file differs.</p> <p>When the client creates the target file, the operation result is as follows: An error about the operation result is not reported.</p> <p>When selecting Allow access</p> <p>The target file can be created newly.</p> <p>When selecting Deny access</p> <p>The target file is deleted and therefore cannot be created newly.</p> <p>When the client views the target file, the operation result is as follows:</p> <p>When selecting Allow access</p> <p>The target file can be viewed.</p> <p>When selecting Deny access</p> <p>The target file access is denied. The target file cannot be viewed.</p> <p>When the client updates the target file, the operation result is as follows: An error about the operation result is not reported.</p> <p>When selecting Allow access</p> <p>The target file can be updated.</p> <p>When selecting Deny access</p>

Item	Description
	The target file status returns to the status before the update and therefore the target file cannot be updated.
Server monitoring interval	Specify the polling interval to confirm the status of the scan server, from 1 to 86,400 seconds.
Cache size of scanning result	<p>Specify the size of the cache that stores the information on files that were determined to be free of infection as the result of a scan, from 1 to 64 MB.</p> <p>1 MB stores an amount of information equivalent to approximately 430 files. Files whose contents have not been changed from the information that is stored in the cache can be directly accessed without a scan.</p> <p>When changing this setting, make sure that real-time scanning is disabled. If you change the setting while real-time scanning is enabled, you need to perform the following to apply the change: disable real-time scanning, enable it again, and then restart the CIFS service.</p> <p>When Symantec scan software, McAfee scan software, or Trend Micro InterScan Web Security Virtual Appliance is used, this item can be displayed and set.</p>
<p>#1: If Trend Micro ServerProtect is used, when a CIFS client modifies a file, virus scanning is performed asynchronously after the modification processing is complete. Therefore, opening or renaming a file might fail because of contention between the processing for accessing modified files and for virus scanning. If an application (such as Microsoft Office) is used that sometimes reopens or renames a file right after it is modified, saving of the files might fail or unnecessary files might remain in the system. Therefore, in this environment, we recommend that you select Read only for Scan timing.</p> <p>#2: When Trend Micro InterScan Web Security Virtual Appliance is used, if an access to a file is blocked due to the scan server setting, the action same as that taken at infected file detection is taken.</p>	

Scanning software page

A system administrator can set the scan software to use in the **Scanning software** page.



Note: Set the same scan software on both nodes. Note that all the registered scan server information is deleted and the scan condition is initialized when the scan software is changed.

To display the **Scanning software** page, click the **Scanning Software** button from the **List of Scanner Servers** page in the **Virus Scan Server Configuration** dialog box.

Table C-153 Items displayed on the Scanning software page

Item	Description
Select scanning software	<p>Sets the scan software to use.</p> <p>Trend Micro ServerProtect Trend Micro ServerProtect is used.</p> <p>InterScan Web Security Virtual Appliance Trend Micro InterScan Web Security Virtual Appliance is used.</p> <p>Symantec Protection Engine The Symantec scanning software is used.</p> <p>McAfee VirusScan Enterprise McAfee scanning software is used.</p>

CIFS Protocol Settings dialog box

In the **CIFS Protocol Settings** dialog box, you can check the hosts or networks for which access to CIFS share is restricted.

To display the **CIFS Protocol Settings** dialog box, open the **Shares** window, and in the **Shares** area click a CIFS share name.

Table C-154 Items displayed in the CIFS Protocol Settings dialog box

Item	Description
Host/network based access restriction	Displays whether to allow or deny access.
CIFS Share Hosts and Networks	Host/Network Displays the hosts or networks for which access to the CIFS share is restricted.
Access permissions	<p>New files</p> <p>Displays the access permissions of Owner, Group, and Other (all users and groups) for creating files in a CIFS share.</p> <p>RW Permit read-write access.</p> <p>RO Permit read-only access.</p> <p>None Do not permit read or write access.</p> <p>Displays -- if the Access permissions setting of the CIFS share is set to Owner only. Displays Unknown if the ACL type of the file system cannot be acquired.</p>

Item	Description
	<p>New directories</p> <p>Displays the access permissions of Owner, Group, and Other (all users and groups) for creating directories in a CIFS share.</p> <p>RW Permit read-write access.</p> <p>RO Permit read-only access.</p> <p>None Do not permit read or write access.</p> <p>Displays -- if the Access permissions setting of the CIFS share is set to Owner only. Displays Unknown if the ACL type of the file system cannot be acquired.</p>

NFS Protocol Settings dialog box

You can check the hosts and networks that can access NFS shares.

To display the **NFS Protocol Settings** dialog box, display the **Shares** window, and then, in the **Shares** area, click the absolute path to the shared directory.

Table C-155 Items displayed in the NFS Protocol Settings dialog box

Item	Description
NFS Share Hosts and Networks	Host/Network Displays the hosts and networks that can access NFS shares.
	Anonymous Mapping Displays the users who access the HDI system from the hosts and networks that can access NFS shares, specified in Host/Network , and are mapped as anonymous users.

Edit Share dialog box

You can change the file share settings. To set the ACL for a created shared directory, use the `dirsetacl` command.

To display the **Edit Share** dialog box, display the **Shares** window, and then, in the **Shares** area, click the line of the file share whose settings you want to edit, and then click the **Edit** button.

Table C-156 Items displayed in the Edit Share dialog box

Item		Description
File system name		Displays the name of the file system that contains the file share whose settings are being changed.
Share name		Displays the share name.
Protocol		Displays the protocol used for a file share. CIFS The CIFS protocol is used. NFS The NFS protocol is used. CIFS and NFS Both the CIFS and NFS protocols are used.
Use namespace	Yes	Select this check box to allocate HCP namespaces to the share. If you assign the namespace of a linked HCP system, the warning threshold for the usage of the file system will be set to 99%. Use the <code>fsfullmsg</code> command to change the warning threshold as needed. Select the Yes check box to display the settings related to namespaces.
Namespace settings	Content sharing	Displays how data is shared with other HDI systems via the linked HCP when the Yes check box is selected for Use namespace . Off Data is being not synchronized with other HDI systems. On (Read-Only) Data in other HDI systems is being referenced as read-only.
	Namespace name	When Content sharing is set to <code>Off</code> , specify a migration-destination namespace name of no more than six characters to be added to the end of the namespace name. You can use alphanumeric characters and hyphens (-). You cannot, however, use a hyphen as the last character.
	Tenant hard quota	When Content sharing is set to <code>Off</code> , the maximum capacity that can be used for the migration-destination tenant is displayed.
	Storage capacity used	When Content sharing is set to <code>Off</code> , the current capacity usage of the migration-destination tenant is displayed.
	Used namespace quota	When Content sharing is set to <code>Off</code> , the current capacity usage of the migration-destination namespace is displayed.

Item		Description	
	Quota	When Content sharing is set to <i>Off</i> , specify the hard quota to be allocated to the migration-destination namespace. Select GB or TB for the unit. Specify a value that is smaller than the value for Tenant hard quota .	
	Synchronize the file share capacity with the namespace quota	<p>Yes</p> <p>When Content sharing is set to <i>Off</i>, select the check box to limit the capacity used per share based on the hard quota of the migration-destination namespace.</p> <p>If you select the Yes check box, the value specified in Quota will be the maximum value for the capacity that can be used in a share.</p>	
	Namespace FQDN	When Content sharing is set to <i>On (Read-Only)</i> , specify the name of the HCP namespace in fully qualified domain name (FQDN) format.	
	External HCP host name	When Content sharing is set to <i>On (Read-Only)</i> , and then the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.	
	Namespace-access account	<p>User</p> <p>When Content sharing is set to <i>On (Read-Only)</i>, specify the user name of the account for viewing the namespace.</p> <p>Password</p> <p>When Content sharing is set to <i>On (Read-Only)</i>, specify the password of the account for viewing the namespace.</p> <p>After specifying the user name and password, click the Test Connection button to check whether connection to HCP is possible.</p>	
Namespace sharing settings	Namespace-access account	Create	Select this to create an account for viewing the migration-destination namespace. You can specify this item when Content sharing is set to <i>Off</i> .
		User	Displays the user name of the account for viewing the namespace.
		Password	Enter the password of the account for viewing the namespace. The entered password is displayed by using asterisks (*).
		Confirm password	Enter the character string you specified for Password . The entered password is displayed by using asterisks (*).
	Replica system name	Specify the system name of the replica HCP system if replication is used at the location of the HCP system.	

Item		Description
		<p>After changing the system name of the replica HCP, click the Test Connection button to check that the system can be connected to the replica HCP system.</p> <p>You can specify this item when Content sharing is set to On (Read-Only).</p>
	External Replica HCP host name	When Replica system name is specified, and then the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the replica HCP system.
	Replica namespace FQDN	When Replica system name is specified, the name of the namespace of the replica HCP system is displayed.
CIFS share options	CIFS share name	<p>Displays CIFS share names.</p> <p>This item is displayed when Protocol is set to CIFS or CIFS and NFS.</p>
	Enable auto creation of home directory	<p>Yes</p> <p>Select this to use the function for automatically creating a home directory in the CIFS share.</p> <p>For a home-directory-roaming file system, the function for automatically creating a home directory is enabled by default. To disable the function, use the <code>cifsedit</code> command.</p>
	Advanced	<p>SMB encryption</p> <p>Specify whether communication with the CIFS client is to be encrypted.</p> <p>The setting for this item is only valid if you select SMB 3.0 for the SMB protocol in CIFS Service Management (Basic) page of the Access Protocol Configuration dialog box. If you select an option other than SMB 3.0 for the SMB protocol, select Disable or set communication with the CIFS client not to be encrypted in the configuration definition of the CIFS service, and then select the Inherit CIFS service default.</p> <p>Inherit CIFS service default</p> <p>Use the CIFS service configuration definitions.</p> <p>Specify settings for each CIFS share</p> <p>Auto: Select this option if communication with the client is to be encrypted only when the client supports encryption.</p> <p>Mandatory: Select this option if communication with the client is always to be encrypted. The clients that do not support SMB 3.0 cannot access CIFS sharing. Only clients that support SMB 3.0 or later can access a CIFS share. Note that</p>

Item		Description		
			<p>clients cannot access a CIFS share by using guest accounts.</p> <p>Disable: Select this option if communication with the client is not to be encrypted.</p> <p>If you select Mandatory or Disable, specify Auto for the CIFS service configuration definition.</p>	
Access control	CIFS	Host/ network based access restriction	<p>Select whether to allow or deny access.</p> <p>Allow: Specify the hosts or networks for which access is allowed.</p> <p>Deny: Specify the hosts or networks for which access is denied.</p> <p>This item is displayed when Protocol is set to CIFS or CIFS and NFS.</p>	
		CIFS Share Hosts and Networks	Host/ Network	Displays the names of the hosts or networks for which access to the CIFS share is restricted.
			Delete button	Deletes the hosts or networks for which access to the CIFS share is restricted.
			Edit button	Edits the hosts or networks for which access to the CIFS share is restricted. The Edit CIFS Share Host or Network dialog box appears (Edit CIFS Share Host or Network dialog box on page C-204).
			Add button	Add the hosts or networks for which access to the CIFS share is restricted. The Add CIFS Share Host or Network dialog box appears (Add CIFS Share Host or Network dialog box on page C-205).
		Access permissions	Owner only	Select this check box to set read or write permissions only to Owner . Access permissions are not set for Group or Other (all users and groups).
			New files	<p>If you did not select Owner only, access permissions for creating files are set for Owner, Group, and Other (all users and groups).</p> <p>RW</p> <p>Select this option to permit read-write access.</p> <p>RO</p> <p>Select this option to permit read-only access.</p>

Item			Description
			<p>None</p> <p>Select this option to not permit read or write access.</p> <p>If RO or None is specified for Owner, even the owner will not be able to write to new files.</p> <p>If RO is set for Group, set RO or None for Other. To set None for Group, also set None for Other. If you set access permissions other than these for Other, Group access permissions set for files might be deleted when the files are updated.</p>
			<p>New directories</p> <p>If you did not select Owner only, set access permissions for creating directories to Owner, Group, and Other (all users and groups).</p> <p>RW</p> <p>Select this option to permit read-write access.</p> <p>RO</p> <p>Select this option to permit read-only access.</p> <p>None</p> <p>Select this option to not permit read or write access.</p> <p>If you specify RO or None for Owner, even the owner will not be able to write to new directories.</p> <p>If you set RO for Group, set RO or None for Other as well. If you set None for Group, set None for Other as well. If you set access permissions other than these for Other, Group access permissions set for directories might be deleted when the directories are updated.</p>
NFS	NFS Share Hosts and Networks	Host/ Network	<p>Displays the hosts and networks that can access the NFS share.</p> <p>This item is displayed when Protocol is set to NFS or CIFS and NFS.</p>
		Anonymous Mapping	<p>Displays the users who access the HDI system from the hosts and networks that can access NFS shares, specified in Host/ Network, and are mapped as anonymous users.</p>

Item			Description	
			Delete button	Deletes an object that can access the NFS share.
			Edit button	Displays the Edit NFS Share Host or Network dialog box that can be used to edit the objects that can access an NFS share (Edit NFS Share Host or Network dialog box on page C-206).
			Add button	Displays the Add NFS Share Host or Network dialog box that can be used to add an object that can access the NFS share (Add NFS Share Host or Network dialog box on page C-207).

Release Share(s) dialog box

You can release file system shares.

To display the **Release Share(s)** dialog box, display the **Shares** window, and then, in the **Shares** area, click the line for the file share to be released, and then click the **Release** button.

Table C-157 Items displayed in the Release Share(s) dialog box

Item		Description
Shares	Share Name	Displays the share name.
	Protocol	Displays the protocol used for the file share.
	File System Name	Displays the name of the file system for which the file share was created.
Apply button		Releases the file share.

Edit CIFS Share Host or Network dialog box

In the **Edit CIFS Share Host or Network** dialog box, you can edit the hosts or networks for which access to CIFS share is restricted.

To display the **Edit CIFS Share Host or Network** dialog box, in the **Edit Share** dialog box, click the **Edit** button in **CIFS Share Hosts and Networks**.

Table C-158 Items displayed in the Edit CIFS Share Host or Network dialog box

Item	Description
Host/Network	<p>Specify the CIFS client host names or network addresses for which access to the CIFS share is to be restricted.</p> <p>Use no more than 5,631 characters.</p> <p>Specify the network address in the format below: <i>network-address/netmask</i> (for example, 10.203.15.0/255.255.255.0)</p> <p>For IPv6, specify a prefix length as the netmask.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If the hosts or networks for which access to the CIFS service is restricted are set in the configuration definitions of the CIFS service (set on the CIFS Service Management (Security) page in the Access Protocol Configuration dialog box), the settings are applied to all file shares. If you want to restrict the access from hosts or networks to individual CIFS shares, do not set the hosts or networks for which access is restricted in the configuration definitions of the CIFS service. • When specifying host names, edit the <code>/etc/hosts</code> file to add all the specified host names and IP addresses. If host names are not added to the <code>/etc/hosts</code> file, the specified information might not be enabled. Of the host names corresponding to the IP addresses, if you specify a host name that has already been added as an alias name for an IP address, the resulting operations might not be as specified. For details about how to edit the <code>/etc/hosts</code> file, see Edit System File page on page C-126. • You cannot specify the following names as the host name: <ul style="list-style-type: none"> - ALL - FAIL - EXCEPT • User authentication for CIFS clients is performed even if access to CIFS share is allowed.

Add CIFS Share Host or Network dialog box

In the **Add CIFS Share Host or Network** dialog box, you can add hosts or networks for which access to CIFS share is allowed or denied.

To display the **Add CIFS Share Host or Network** dialog box, in the **Edit Share** dialog box, click the **Add** button in **CIFS Share Hosts and Networks**.

Table C-159 Items displayed in the Add CIFS Share Host or Network dialog box

Item	Description
Host/Network	<p>Specify CIFS client host names or network addresses for which access to the CIFS share is restricted.</p> <p>For details about how to set the information, in the Edit CIFS Share Host or Network dialog box, see the description in Host/Network (Edit CIFS Share Host or Network dialog box on page C-204).</p>

Edit NFS Share Host or Network dialog box

You can change the hosts or networks that can access an NFS share.

To display the **Edit NFS Share Host or Network** dialog box, click the **Edit** button for **NFS Share Hosts and Networks** in the **Edit Share** dialog box.

Table C-160 Items displayed in the Edit NFS Share Host or Network dialog box

Item	Description
Host/Network	<p>Specify the host or network address that you want to allow to access the NFS share.</p> <p>Specify 255 characters or fewer. Specify a host name beginning with an alphabetic character and consisting of alphanumeric characters, hyphens (-), and underscores (_). If you specify a host alias, the official host name also must be 255 characters or fewer.</p> <p>Note that the total length (specified length + 5 bytes) of the specified host names or network addresses must be less than 1,258 bytes.</p> <p>In addition to the host name and the IP address, you can use the following formats:</p> <p>Netgroup Specify an NIS netgroup. For example, for @group, only the host segment is extracted from the netgroup members.</p> <p>IP network To permit all hosts in the subnetwork to access the NFS share, specify the IP address and the netmask in the following format: <i>address/netmask</i></p> <p>The netmask can be specified with decimal numbers separated by a period (.) or with the prefix length (for IPv6, the netmask can only be specified with the prefix length).</p> <p>DNS domain Specify the name of the DNS domain to which NFS clients belong, with a period (.) added at the beginning of the name. Example: .example.com</p> <p>Wild card</p>

Item	Description
	<p>To specify all hosts, use an asterisk (*) as a wild card.</p> <p>When the NFS client machine has multiple network interfaces communicating with the HDI system, specify the hosts and networks allowed to access the NFS share in one of the following formats:</p> <ul style="list-style-type: none"> • Use a wild card (*). • Specify the IP addresses of all network interfaces used on the NFS client side. • Specify the host names for all network interfaces used on the NFS client side. • Specify an IP network that contains the IP addresses of all network interfaces used on the NFS client side. • Specify a netgroup that contains the host names for all network interfaces used on the NFS client side. • Specify a DNS domain that contains the host names for all network interfaces used on the NFS client side.
Anonymous mapping	<p>Select users who can access the HDI system from the hosts allowed to access the NFS share specified in the Host/Network and those you want to map as anonymous users.</p> <p>Not applied Select this option to disable anonymous user mapping.</p> <p>For root user Select this option to map only the root user as an anonymous user.</p> <p>For anyone Select this option to map every user as an anonymous user.</p>

Add NFS Share Host or Network dialog box

You can add hosts or networks that can access the NFS share.

To display the **Add NFS Share Host or Network** dialog box, click the **Add** button for **NFS Share Hosts and Networks** in the **Edit Share** dialog box.

Table C-161 Items displayed in the Add NFS Share Host or Network dialog box

Item	Description
Host/Network	<p>Specify the host or network that you want to allow to access the NFS share.</p> <p>For details about how to specify the host or network, see the description of Host/Network in the Edit NFS Share Host or Network dialog box (Edit NFS Share Host or Network dialog box on page C-206).</p>
Anonymous mapping	<p>Select users who can access the HDI system from the hosts allowed to access the NFS share specified in the Host/Network and those you want to map as anonymous users.</p>

Item	Description
	<p>Not applied Select this option to disable anonymous user mapping.</p> <p>For root user Select this option to map only the root user as an anonymous user.</p> <p>For anyone Select this option to map every user as an anonymous user.</p>

Add Share dialog box

You can add a file share in the file system.

A maximum of 1,024 NFS shares can be created.

The maximum number of CIFS shares varies depending on whether the configuration definition of the CIFS service is set so that the settings on CIFS shares are automatically reloaded and applied to the CIFS client environment. For details about the maximum number of CIFS shares, see the *File System Protocols (CIFS/NFS) Administrator's Guide*.

To display the **Add Share** dialog box, display the **File Systems** window, and then, in the **File Systems** tab, select the line for the file system in which you want to add a file share, and then click the **Add Share** button.

Table C-162 Items displayed in the Add Share dialog box

Item	Description
File system name	Displays the name of the file system to which a file share is being added.
Share directory	Specifies the shared directory name. This item is not displayed if you create a read-write-content-sharing file system or home-directory-roaming file system. The mount point is automatically specified as the shared directory.
Share name	Displays the share name.
Protocol	Specifies the protocol to be used for the file share being added. CIFS The CIFS protocol will be used. NFS The NFS protocol will be used. CIFS and NFS Both the CIFS and NFS protocols will be used.

Item		Description
		If you create a file share in a home-directory-roaming file system, CIFS is specified automatically.
Directory to use	Use existing directory as is	Select this to use an existing directory as a shared directory without changing any permission settings. If you create a file share in a read-write-content-sharing file system or home-directory-roaming file system, this item is not displayed because the mount point is specified as the shared directory.
	Create directory	Select this to create a new directory as a shared directory or to change the permission settings of the existing directory that is to be used as a shared directory. If this item is selected, <code>root</code> is set as the user and group names. If you create a file share in a read-write-content-sharing file system or home-directory-roaming file system, this item is not displayed because the mount point is specified as the shared directory.
Use namespace	Yes	Select this check box to add a file share directly below the mount point for the file system, and then allocate the HCP namespace to the file share. If you assign the namespace of a linked HCP system, the warning threshold for the usage of the file system will be set to 99%. Use the <code>fsfullmsg</code> command to change the warning threshold as needed. Select the Yes check box to display the settings related to namespaces.
Namespace settings	Content sharing	Displays how data is shared with other HDI systems via the linked HCP when the Yes check box is selected for Use namespace . <code>Off</code> Data is being not synchronized with other HDI systems. <code>On (Read-Only)</code> Data in other HDI systems is being referenced as read-only.
	Namespace name	When Content sharing is set to <code>Off</code> , specify a migration-destination namespace name of no more than six characters to be added to the end of the namespace name. You can use alphanumeric characters and hyphens (-). You cannot, however, use a hyphen as the last character.
	Tenant hard quota	When Content sharing is set to <code>Off</code> , the maximum capacity that can be used for the migration-destination tenant is displayed.

Item		Description	
	Storage capacity used	When Content sharing is set to <code>Off</code> , the current capacity usage of the migration-destination tenant is displayed.	
	Quota	When Content sharing is set to <code>Off</code> , specify the hard quota to be assigned to the migration-destination namespace. Specify the quota to be assigned to the namespace in GB or TB units. Specify a value that is smaller than the value for Tenant hard quota .	
	Synchronize the file share capacity with the namespace quota	<p>Yes</p> <p>When Content sharing is set to Off, select the check box to limit the capacity used per share based on the hard quota of the migration-destination namespace.</p> <p>If you select the Yes check box, the value specified in Quota will be the maximum value for the capacity that can be used in a share.</p>	
	Namespace FQDN	When Content sharing is set to <code>On (Read-Only)</code> , specify the name of the HCP namespace in fully qualified domain name (FQDN) format.	
	External HCP host name	When Content sharing is set to <code>On (Read-Only)</code> , and then the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.	
	Namespace-access account	<p>User</p> <p>When Content sharing is set to <code>On (Read-Only)</code>, specify the user name of the account used to view the namespace.</p> <p>Password</p> <p>When Content sharing is set to <code>On (Read-Only)</code>, specify the password of the account for viewing the namespace.</p> <p>After specifying the user name and password, click the Test Connection button to check whether connection to HCP is possible.</p>	
Namespace sharing settings	Namespace-access account	Create	Select this to create an account for viewing the migration-destination namespace. You can specify this item when Content sharing is set to <code>Off</code> .
		User	Displays the user name of the account for viewing the namespace.
		Password	Enter the password of the account for viewing the namespace. The entered password is displayed by using asterisks (*).
		Confirm password	Enter the character string you specified for Password .

Item		Description
		The entered password is displayed by using asterisks (*).
	Replica system name	Specify the system name of the replica HCP system if replication is used at the location of the HCP system. After changing the system name of the replica HCP, click the Test Connection button to check that the system can be connected to the replica HCP system. You can specify this item when Content sharing is set to <code>On (Read-Only)</code> .
	External Replica HCP host name	When Replica system name is specified, and then the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the replica HCP system.
	Replica namespace FQDN	When Replica system name is specified, the name of the namespace of the replica HCP system is displayed.
CIFS share options	CIFS share name	Specify the CIFS share name. This item is displayed if either CIFS or CIFS and NFS is selected for Protocol .
	Enable auto creation of home directory	Yes Select this to use the function for automatically creating a home directory in the CIFS share. When creating a file share in a home-directory-roaming file system, the function for automatically creating a home directory is enabled by default. To disable the function, use the <code>cifseddit</code> command.
	Advanced	SMB encryption Specify whether communication with the CIFS client is to be encrypted. The setting for this item is only valid if you select SMB 3.0 for the SMB protocol in CIFS Service Management (Basic) page of the Access Protocol Configuration dialog box. If you select an option other than SMB 3.0 for the SMB protocol , select Disable or set communication with the CIFS client not to be encrypted in the configuration definition of the CIFS service, and then select the Inherit CIFS service default . Inherit CIFS service default Use the CIFS service configuration definitions. Specify settings for each CIFS share Auto: Select this option if communication with the client is to be encrypted only when the client supports encryption.

Item		Description		
			<p>Mandatory: Select this option if communication with the client is always to be encrypted. The clients that do not support SMB 3.0 cannot access CIFS sharing. Only clients that support SMB 3.0 or later can access a CIFS share. Note that clients cannot access a CIFS share by using guest accounts.</p> <p>Disable: Select this option if communication with the client is not to be encrypted.</p> <p>If you select Mandatory or Disable, specify Auto for the CIFS service configuration definition.</p>	
Access control	CIFS	Host/network based access restriction	<p>Select whether to allow or deny access.</p> <p>Allow: Specify the hosts or networks for which access is allowed.</p> <p>Deny: Specify the hosts or networks for which access is denied.</p> <p>This item is displayed when CIFS or CIFS and NFS is selected for the Protocol.</p>	
		CIFS Share Hosts and Networks	Host/Network	Displays the names of hosts or networks for which access to the CIFS share is restricted.
			Delete button	Delete the hosts or networks for which access to the CIFS share is restricted.
			Edit button	Displays the Edit CIFS Share Host or Network dialog box that can be used to edit the hosts or networks for which access to the CIFS share is restricted (Edit CIFS Share Host or Network dialog box on page C-204).
			Add button	Displays the Add CIFS Share Host or Network dialog box that can be used to add hosts or networks for which access to the CIFS share is restricted (Add CIFS Share Host or Network dialog box on page C-205).
		Access permissions	Owner only	Select this check box to set read or write permissions only to Owner . Access permissions are not set for Group or Other (all users and groups).
New files	If you did not select Owner only , access permissions for creating files are set for Owner , Group , and Other (all users and groups). RW			

Item			Description	
				<p>Select this option to permit read-write access.</p> <p>RO</p> <p>Select this option to permit read-only access.</p> <p>None</p> <p>Select this option to not permit read or write access.</p> <p>If RO or None is specified for Owner, even the owner will not be able to write to new files.</p> <p>If RO is set for Group, set RO or None for Other. To set None for Group, also set None for Other. If you set access permissions other than these for Other, Group access permissions set for files might be deleted when the files are updated.</p>
			New directories	<p>If you did not select Owner only, set access permissions for creating directories to Owner, Group, and Other (all users and groups).</p> <p>RW</p> <p>Select this option to permit read-write access.</p> <p>RO</p> <p>Select this option to permit read-only access.</p> <p>None</p> <p>Select this option to not permit read or write access.</p> <p>If you specify RO or None for Owner, even the owner will not be able to write to new directories.</p> <p>If you set RO for Group, set RO or None for Other as well. If you set None for Group, set None for Other as well. If you set access permissions other than these for Other, Group access permissions set for directories might be deleted when the directories are updated.</p>
	NFS	NFS Share Hosts and Networks	Host/ Network	<p>Displays the hosts and networks that can access the NFS share.</p> <p>This item is displayed when NFS or CIFS and NFS is selected for the Protocol.</p>
			Anonymous Mapping	<p>Displays the users who access the HDI system from the hosts and</p>

Item		Description	
			networks that can access NFS shares, specified in Host/Network , and are mapped as anonymous users.
		Delete button	Deletes an object that can access the NFS share.
		Edit button	Displays the Edit NFS Share Host or Network dialog box that can be used to change the objects that can access the NFS share (Edit NFS Share Host or Network dialog box on page C-206).
		Add button	Displays the Add NFS Share Host or Network dialog box that can be used to add an object that can access the NFS share (Add NFS Share Host or Network dialog box on page C-207).
Directory	ACL type		Displays the ACL type of the file system. Advanced ACL The ACL type is Advanced ACL. Classic ACL The ACL type is Classic ACL. This item is displayed when Create directory is selected for Directory to use .
		ACL Registered Users and Groups	Type Displays the type of the target user or group. Items related to ACL Registered Users and Groups are displayed when ACL type is set to <i>Advanced ACL</i> .
		Name Displays the name of the target user or group.	
		Account Type Displays whether the account has been registered as a user or group.	
		Permissions Displays the operations for which access is allowed or denied.	
		Apply to Displays whether the ACL settings are also applied to the subfolders and files as well as this folder (shared directory).	
		Setting button Displays the Advanced ACL Settings dialog box that can be used to set ACLs to the shared directory (Advanced ACL Settings dialog box on page C-235).	

Item		Description
	Export point	Displays the access permissions to the shared directory for Owner , Group , and Other . Items related to Export point are displayed when ACL type is set to <code>Classic ACL</code> .
	Export point owner user	Displays the owner of the shared directory.
	Export point owner group	Displays the owner group of the shared directory.
	Export point permissions	Sets the access permissions to the shared directory for Owner , Group , and Other . RW Select this option when you allow read, write, and execution permissions to the shared directory. RO Select this option when you allow read and execution permissions to the shared directory. None Select this option when you do not allow read, write, and execute permissions to the directory.
	Unix sticky bit	Yes Select the Yes check box to set a sticky bit for the shared directory.

Create File System dialog box

You can create a new file system.

To display the **Create File System** dialog box, display the **File Systems** window, and then, click the **Create** button.



Tip: The recommended number of file systems is four (but up to 256 file systems can be created).

Table C-163 Items displayed in the Create File System dialog box

Item	Description
File system name	Specify the name of the file system you want to create.

Item	Description		
Namespace type	<p>Specify how to link to the HCP system. If you assign the namespace of a linked HCP system, the warning threshold for the usage of the file system will be set to 99%. Use the <code>fsfullmsg</code> command to change the warning threshold as needed.</p> <p>File system The file system is linked to the HCP system at the file system level.</p> <p>Subtree The file system is linked to the HCP system at the share level. If you select Subtree, a file system of the Advanced ACL type will be created.</p> <p>None An HCP namespace is not used. This item is displayed when HCP information is not set.</p>		
Protocol	<p>Specify the protocol to be used for the file system.</p> <p>CIFS Indicates that the CIFS protocol is to be used. Make sure to select CIFS when you select Home directory for Content sharing.</p> <p>NFS Indicates that the NFS protocol is to be used.</p> <p>CIFS and NFS Indicates that the CIFS and NFS protocols are to be used. This item is not displayed when Namespace type is set to Subtree.</p>		
Namespace settings	Content sharing	<p>Specify how data is to be shared with other HDI systems via the linked HCP.</p> <p>Off Data is not synchronized with other HDI systems.</p> <p>On (Read-Only) Data in other HDI systems is referenced as read-only.</p> <p>On (Read/Write) Data is shared among HDI systems by using the read-write-content-sharing functionality. Select File system for Namespace type.</p> <p>Home directory Roaming among HDI systems is enabled for home directory data created for each end user. This item can be specified when Protocol is set to CIFS. In addition, select File system for Namespace type.</p>	
	Create namespace	Yes	<p>Select this check box when Content sharing is set to On (Read/Write) or Home directory and a migration-destination namespace is created.</p> <p>When you use an existing namespace, do not select this check box, but specify the name of the migration-destination namespace for Namespace name.</p>

Item	Description	
Tenant hard quota	<p>Displays the maximum capacity that can be used for the migration-destination tenant.</p> <p>This item is displayed when either of the following conditions exists:</p> <ul style="list-style-type: none"> • Namespace type is set to File system and Content sharing is set to Off • Content sharing is set to On (Read/Write) or Home directory and the Create namespace check box is selected. 	
Storage capacity used	<p>Displays the current capacity usage of the migration-destination tenant.</p> <p>This item is displayed when either of the following conditions exists:</p> <ul style="list-style-type: none"> • Namespace type is set to File system and Content sharing is set to Off • Content sharing is set to On (Read/Write) or Home directory and the Create namespace check box is selected. 	
Quota	<p>Specify the hard quota to be assigned to the migration-destination namespace. Specify the quota to be assigned to the namespace in GB or TB units. Specify a value that is smaller than the value for Tenant hard quota.</p> <p>This item is displayed when either of the following conditions exists:</p> <ul style="list-style-type: none"> • Namespace type is set to File system and Content sharing is set to Off • Content sharing is set to On (Read/Write) or Home directory and the Create namespace check box is selected. 	
Namespace FQDN	<p>Specify the name of the HCP namespace in fully qualified domain name (FQDN) format.</p> <p>This item is displayed when Namespace type is set to File system and Content sharing is set to On (Read-Only).</p>	
External HCP host name	<p>If the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.</p> <p>This item is displayed when Namespace type is set to File system and Content sharing is set to On (Read-Only).</p>	
Namespace-access account	User	<p>Specify the user name of the account used to view the HCP namespace.</p> <p>Items related to Namespace-access account are displayed when Namespace type is set to File system and Content sharing is set to On (Read-Only).</p>
	Password	<p>Specify the password of the account used to view the namespace.</p>

Item	Description		
			After specifying the user name and password, click the Test Connection button to check whether connection to HCP is possible.
	Namespace name		<p>When Content sharing is set to On (Read/Write) or Home directory, if you want to use an existing namespace, use the drop-down list or text box to specify the name of the migration-destination namespace.</p> <p>After you specify a namespace name, click the Test Connection button to check whether the namespace is accessible.</p> <p>When Content sharing is set to On (Read/Write), If a list of namespaces cannot be obtained from the HCP system, no space name can be selected and an error message is displayed. In such a case, revise the settings for connections to the HCP system, and then redisplay the Create File System dialog box.</p>
Migration schedule	Start date		<p>Specify the first date on which migration is to be executed. Click the calendar icon, and then click a date in the displayed calendar.</p> <p>You can specify items related to Migration schedule when Content sharing is set to Off.</p>
	Regular task scheduling	Interval	<p>Specify the migration interval. Move the slider on the bar that indicates the interval to specify an interval in the range from 15 minutes to 1 week.</p> <p>The currently set interval is displayed on the bar in the following format: Every numerical-value <minute(s), hour(s), day(s), or week></p>
		Start time	Specify the start time of the migration.
		Maximum duration	Specify how long migration processing can continue.
Cache settings	Storage system		<p>Select the storage destination (internal hard disk or storage system) for the data in the file system when multiple volume groups exist. Storage systems that can be selected are displayed in a drop-down list in the following format: <i>storage-system-model-name serial-number</i></p> <p>For internal hard disks, <code>INTERNAL</code> is displayed for the model name.</p>
	Volume group		<p>Select a volume group to be used by the file system when multiple volume groups exist. Volume groups that can be selected are displayed in a drop-down list in the following format: <i>volume-group-name total-capacity-of-volume-group (maximum-capacity-that-can-be-allocated-to-file-system Available) drive-type</i></p>
	Unallocated capacity		Displays the capacity that can be allocated to the file system when one volume group exists.

Item	Description		
	Capacity	<p>Specify the capacity to be allocated to the file system in GB or TB units.</p> <p>The upper limit for expansion of the file system capacity is also displayed on the right-hand side. If the initial capacity of a created file system is equal to or less than 32 GB, the maximum capacity after expansion will be less than the displayed value. For details about the initial capacity of a created file system and the maximum capacity after expansion, see the <i>CLI Administrator's Guide</i>.</p> <p>If you use the Large File Transfer function, specify 140 GB or more.</p> <p>Part of the specified size will be used as the work space for the Active File Migration function and the Large File Transfer function. For details about the size of the work space to be allocated for a specified file system capacity, see Table 3-1 Size of the work space to be used by the Active File Migration function and the Large File Transfer function on page 3-2 or Table 3-2 Size of the work space to be used by the Active File Migration function (when the Large File Transfer function is not used) on page 3-2.</p>	
Namespac e sharing settings	Namespac e-access account	Create	<p>Select this to create an account for viewing the migration-destination namespace.</p> <p>You can specify this when Namespace type is set to File system and Content sharing is set to Off.</p>
		User	<p>When Create is selected for Namespace-access account, the user name of the account for viewing the namespace is displayed.</p>
		Password	<p>Enter the password of the account for viewing the namespace.</p> <p>The entered password is displayed by using asterisks (*).</p>
		Confirm password	<p>Enter the character string you specified for Password.</p> <p>The entered password is displayed by using asterisks (*).</p>
	Replica system name	<p>Specify the system name of the replica HCP system if replication is used at the location of the HCP system.</p> <p>After specifying the system name of the replica HCP system, click the Test Connection button to check that the system can be connected to the replica HCP system.</p> <p>You can specify this when Namespace type is set to File system and Content sharing is set to On (Read-Only).</p>	
External Replica HCP host name	<p>When Replica system name is specified, and then the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the replica HCP system.</p>		

Item	Description			
	Replica namespace FQDN	When Replica system name is specified, the name of the namespace of the replica HCP system is displayed.		
File system settings	Enable the WORM function	Yes	<p>Select this to set the WORM function for the file system.</p> <p>Note that after creating a file system, you can no longer change the setting for whether the WORM functionality is enabled or disabled.</p> <p>When linked with an HCP system, the WORM settings items are displayed only if Content sharing is set to Off.</p>	
		Auto commit	Switches between displaying or hiding the setting items for autocommit.	
		Enable	Yes	<p>Select this to enable autocommit for the file system.</p> <p>Note that if you enable autocommit, you can no longer disable it.</p>
			Commit mode	<p>Select the mode of autocommit according.</p> <p>Manual</p> <p>Select this to enable autocommit in manual mode.</p> <p>In manual mode, files that are specified as read-only files by clients are subject to the autocommit functionality.</p> <p>Auto</p> <p>Select this to enable autocommit in auto mode.</p> <p>In auto mode, all ordinary files, except for the system files and files in the system directories, are subject to the autocommit functionality.</p>
			Time until committed	<p>Specify the time until autocommit is performed. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) spin boxes.</p> <p>After you have specified the setting, you cannot change it.</p>
			Default retention period	Specify the default retention period. Specify a value from 1

Item	Description		
			<p>minute to 36,500 days in the day(s), hour(s), and minute(s) spin boxes.</p> <p>Select Infinite to set an unlimited default retention period.</p>
	Enable rename of empty directories	Yes	<p>Select this to allow renaming of empty directories in a WORM file system.</p>
Optimize for Large file transfer	Yes	<p>Select this to use the Large File Transfer function.</p> <p>This item is displayed if Content sharing is Off.</p> <p>This item is displayed if the version of linked HCP system is 8.0 or later.</p> <p>If Yes is selected for a file system for which the Active File Migration function has been disabled, the Active File Migration function is also enabled, which might negatively affect performance during file system accesses.</p>	
	Lower limit of the file size	<p>Specify the lower threshold for the size of files to which the Large File Transfer function is applied. A value in the range from 50 MB to 5 TB can be specified. MB, GB, or TB can be selected as the unit.</p> <p>This item can be specified in cases where Off is selected for Content sharing and Yes is selected for Optimize for Large file transfer.</p> <p>This item is displayed if the version of linked HCP system is 8.0 or later.</p>	
Use file version restore	Yes	<p>Select this to make the past version files (past version directories) migrated to the HCP system available to clients. In addition, select how past-version directories are to be kept in the <code>.history</code> directory.</p> <p>You can specify items related to file version restore only if Content sharing is set to a selection other than On (Read-Only).</p>	
	Custom schedule	<p>Select this if you want to use a custom schedule for keeping past-version directories. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p>	
		Schedule settings	<p>Configure a custom schedule.</p> <ul style="list-style-type: none"> • Keep 15-MINUTE versions for: The oldest past version directory with 15-minute

Item	Description			
				<p>time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60. When Content sharing is set to Home directory, only 60 can be specified.</p> <ul style="list-style-type: none"> • Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48. • Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to 23:59) is kept for the number of units specified. Specify in the range from 1 to 62. • Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 156. • Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 72. • Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.
		<p>Period to hold[#]</p>		<p>Select this if you want to keep past-version directories for each migration interval. Specify a value between 1 and 36,500 for the number of days for which the past-version directories are to be kept.</p>

Item	Description		
	CIFS bypass traverse checking	Enable	<p>Select this to enable CIFS bypass traverse checking.</p> <p>This item is not displayed when Content sharing is set to Home directory.</p>
Share settings	Share directory	<p>Specify the name of the shared directory.</p> <p>This item is not displayed when Content sharing is set to On (Read/Write) or Home directory. The mount point is automatically specified as the shared directory.</p> <p>Items related to Share settings do not appear if Namespace type is set to Subtree. Use the Add Share dialog box to add a file share (Add Share dialog box on page C-208).</p>	
	Share name	Displays the share name.	
	CIFS share options	CIFS share name	<p>Specifies the CIFS share name.</p> <p>This item is displayed if either CIFS or CIFS and NFS is selected for Protocol.</p>
		Enable auto creation of home directory	<p>Yes</p> <p>Select this to use the function for automatically creating a home directory in the CIFS share.</p> <p>When Content sharing is set to Home directory, the function for automatically creating a home directory is enabled by default. To disable the function, use the <code>cifsedit</code> command.</p>
		Advanced	SMB encryption

Item	Description			
				<p>client is to be encrypted only when the client supports encryption.</p> <p>Mandatory: Select this option if communication with the client is always to be encrypted. The clients that do not support SMB 3.0 cannot access CIFS sharing. Only clients that support SMB 3.0 or later can access a CIFS share. Note that clients cannot access a CIFS share by using guest accounts.</p> <p>Disable: Select this option if communication with the client is not to be encrypted.</p> <p>If you select Mandatory or Disable, specify Auto for the CIFS service configuration definition.</p>
Access control	CIFS	Host/network based access restriction	<p>Select whether to allow or deny access.</p> <p>Allow: Specify the hosts or networks for which access is allowed.</p> <p>Deny: Specify the hosts or networks for which access is denied.</p> <p>This item is displayed if either CIFS or CIFS and NFS is selected for Protocol.</p>	
		CIFS Share Hosts and Networks	Host/Network	Displays the names of hosts or networks for which access to CIFS shares is restricted.
	Delete button	Delete the hosts or networks for which access to CIFS shares is restricted.		
	Edit button	Displays the Edit CIFS Share Host or Network dialog box that can be used to edit the hosts or networks for which access to CIFS shares is restricted (Edit CIFS Share Host or Network dialog box on page C-204).		
	Add button	Displays the Add CIFS Share Host or Network dialog box that can be used to add hosts or networks for which access to CIFS shares is restricted (Add CIFS Share Host or Network dialog box on page C-205).		

Item	Description		
		Access permissions	<p>Select this check box to set read or write permissions only to Owner. Access permissions are not set for Group or Other (all users and groups).</p>
		New files	<p>If you did not select Owner only, access permissions for creating files are set for Owner, Group, and Other (all users and groups).</p> <p>RW Select this option to permit read-write access.</p> <p>RO Select this option to permit read-only access.</p> <p>None Select this option to not permit read or write access.</p> <p>If RO or None is specified for Owner, even the owner will not be able to write to new files.</p> <p>If RO is set for Group, set RO or None for Other. To set None for Group, also set None for Other. If you set access permissions other than these for Other, Group access permissions set for files might be deleted when the files are updated.</p>
		New directories	<p>If you did not select Owner only, set access permissions for creating directories to Owner, Group, and Other (all users and groups).</p> <p>RW Select this option to permit read-write access.</p> <p>RO Select this option to permit read-only access.</p> <p>None Select this option to not permit read or write access.</p> <p>If you specify RO or None for Owner, even the owner will not be able to write to new directories.</p>

Item	Description			
				If you set RO for Group , set RO or None for Other as well. If you set None for Group , set None for Other as well. If you set access permissions other than these for Other , Group access permissions set for directories might be deleted when the directories are updated.
	NFS	NFS Share Hosts and Networks	Host/ Network	Displays the hosts and networks that can access NFS shares. This item is displayed when NFS or CIFS and NFS is selected for the Protocol .
			Anonymous Mapping	Displays the users who access the HDI system from the hosts and networks that can access NFS shares, specified in Host/ Network , and are mapped as anonymous users.
			Delete button	Deletes an object that can access NFS shares.
			Edit button	Displays the Edit NFS Share Host or Network dialog box that can be used to change the objects that can access NFS shares (Edit NFS Share Host or Network dialog box on page C-206).
			Add button	Displays the Add NFS Share Host or Network dialog box that can be used to add an object that can access NFS shares (Add NFS Share Host or Network dialog box on page C-207).
	Directory	ACL type	Displays the ACL type of the file system. Advanced ACL The ACL type is Advanced ACL. Classic ACL The ACL type is Classic ACL. Items related to Directory do not appear if Namespace type is set to Subtree or if Content sharing is set to Home directory . Items related to Directory appear if Content sharing is set to On (Read/Write) and the Create namespace check box is selected.	
		ACL Registered	Type	Displays the types of target users and groups.

Item	Description	
	Users and Groups	This item is displayed when CIFS or CIFS and NFS is selected for the Protocol .
		Name Displays the names of target users or groups.
		Account Type Displays whether the account has been registered as a user or group.
		Permissions Displays the operations for which access is allowed or denied.
		Apply to Displays whether the ACL settings are also applied to the subfolders and files as well as this folder (shared directory).
		Setting button Displays the Advanced ACL Settings dialog box that can be used to set ACLs to the shared directory (Advanced ACL Settings dialog box on page C-235).
	Export point	Displays the access permissions to the shared directory for Owner , Group , and Other . This item is displayed when NFS is selected for Protocol .
	Export point owner user	Displays the owner of the shared directory.
	Export point owner group	Displays the owner group of the shared directory.
	Export point permissions	Sets the access permissions to the shared directory for Owner , Group , and Other . RW Select this option when you allow read, write, and execution permissions to the shared directory. RO Select this option when you allow read and execution permissions to the shared directory. None Select this option when you do not allow read, write, and execute permissions to the directory.
	Unix sticky bit	Yes Select the Yes check box to set a sticky bit for the shared directory.

Item	Description
	#: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i> .

Edit File System dialog box

You can change file system settings.

To display the **Edit File System** dialog box, display the **File Systems** window, and then, in the **File Systems** tab, click the line for the file system whose setting you want to change, and then click the **Edit** button.

Table C-164 Items displayed in the Edit File System dialog box

Item	Description								
File system name	Displays the name of the file system whose setting you want to change.								
Namespace name	Displays the name of the namespace allocated to the file system when data is migrated to the HCP system at the file system level.								
Task name	Displays the task set for each file system.								
Namespace type	<p>Displays how the file system is linked to the HCP system.</p> <p>If you want to change the file system settings to migrate data to the HCP system, specify how to link to the HCP system. If you assign the namespace of a linked HCP system, the warning threshold for the usage of the file system will be set to 99%. Use the <code>fsfullmsg</code> command to change the warning threshold as needed.</p> <p>File system The file system is linked to the HCP system at the file system level.</p> <p>Subtree The file system is linked to the HCP system at the share level.</p> <p>None An HCP namespace is not used.</p>								
Namespace settings	<table border="1"> <thead> <tr> <th>Content sharing</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Off</td> <td>Data is not being synchronized with other HDI systems.</td> </tr> <tr> <td>On (Read-Only)</td> <td>Data in other HDI systems is being referenced as read-only.</td> </tr> <tr> <td>On (Read/Write)</td> <td>Data is being shared among HDI systems by using the read-write-content-sharing functionality (read-write-content-sharing file system).</td> </tr> </tbody> </table>	Content sharing	Description	Off	Data is not being synchronized with other HDI systems.	On (Read-Only)	Data in other HDI systems is being referenced as read-only.	On (Read/Write)	Data is being shared among HDI systems by using the read-write-content-sharing functionality (read-write-content-sharing file system).
Content sharing	Description								
Off	Data is not being synchronized with other HDI systems.								
On (Read-Only)	Data in other HDI systems is being referenced as read-only.								
On (Read/Write)	Data is being shared among HDI systems by using the read-write-content-sharing functionality (read-write-content-sharing file system).								

Item	Description	
	<p>Home directory</p> <p>Roaming among HDI systems is enabled for home directory data created for each end user (home-directory-roaming file system).</p> <p>If the way to link to the HCP system is specified for Namespace type, <i>Off</i> is set.</p>	
Tenant hard quota	<p>The maximum capacity that can be used for the migration-destination tenant is displayed.</p> <p>This item is displayed when Namespace type is set to <i>File system</i> and Content sharing is set to a selection other than <i>On (Read-Only)</i>.</p>	
Storage capacity used	<p>The current capacity usage of the migration-destination tenant is displayed.</p> <p>This item is displayed when Namespace type is set to <i>File system</i> and Content sharing is set to a selection other than <i>On (Read-Only)</i>.</p>	
Used namespace quota	<p>The capacity used by the migration-destination namespace is displayed.</p> <p>This item is displayed when Namespace type is set to <i>File system</i> and Content sharing is set to a selection other than <i>On (Read-Only)</i>.</p>	
Quota	<p>Specify the hard quota to be allocated to the migration-destination namespace. Select GB or TB for the unit. Specify a value that is smaller than the value for Tenant hard quota.</p> <p>This item is displayed when Namespace type is set to <i>File system</i> and Content sharing is set to a selection other than <i>On (Read-Only)</i>.</p>	
Namespace FQDN	<p>The name of the HCP namespace is displayed.</p> <p>This item is displayed when Namespace type is set to <i>File system</i> and Content sharing is set to <i>On (Read-Only)</i>.</p>	
External HCP host name	<p>If the HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the HCP system.</p> <p>This item is displayed when Namespace type is set to <i>File system</i> and Content sharing is set to <i>On (Read-Only)</i>.</p>	
Namespace-access account	User	<p>Specify the user name of the account for viewing the namespace.</p> <p>Items related to Namespace-access account are displayed when Namespace type is set to <i>File system</i> and Content sharing is set to <i>On (Read-Only)</i>.</p>
	Password	<p>Specify the password of the account for viewing the HCP namespace.</p>

Item	Description		
			<p>After specifying the user name and password, click the Test Connection button to check whether connection to HCP is possible.</p> <p>This item is displayed when Namespace type is set to <code>File system</code> and Content sharing is set to <code>On (Read-Only)</code>.</p>
Migration schedule	Start date	<p>Specify the first date on which migration is to be executed. Click the calendar icon, and then click a date in the displayed calendar.</p> <p>You can specify items related to Migration schedule when Content sharing is set to <code>Off</code>.</p>	
	Regular task scheduling	Interval	<p>Specify the migration interval. Move the slider on the bar that indicates the interval to specify an interval in the range from 15 minutes to 1 week.</p> <p>The currently set interval is displayed on the bar in the following format: Every numerical-value <minute(s), hour(s), day(s), or week></p>
		Start time	Specify the start time of the migration.
		Maximum duration	Specify how long migration processing is allowed to continue.
Cache settings	Storage system	Displays the storage destination for the data in the file system when multiple volume groups exist.	
	Volume group	Displays the volume group being used by the file system when multiple volume groups exist.	
	Unallocated capacity	Displays the capacity that can be allocated to the file system when one volume group exists.	
	Capacity^{#1}	<p>Specify the capacity to be allocated to the file system in GB or TB units.</p> <p>The upper limit for expansion of the file system capacity is also displayed on the right-hand side. If the initial capacity of a created file system is equal to or less than 32 GB, the maximum capacity after expansion will be less than the displayed value. For details about the initial capacity of a created file system and the maximum capacity after expansion, see the <i>CLI Administrator's Guide</i>.</p> <p>If you use the Large File Transfer function, specify 140 GB or more.</p> <p>Part of the specified size will be used as the work space for the Active File Migration function and the Large File Transfer function. For details about the size of the work space to be allocated for a specified file system capacity, see Table 3-1 Size of the work space to be used by the Active File Migration function and the Large File Transfer function on page 3-2 and Table 3-2 Size of the work space to be used by the Active File Migration function (when the Large File Transfer function is not used) on page 3-2.</p>	

Item	Description		
Namespace sharing settings	Namespace access account	Create	Select this to create an account for viewing the migration-destination namespace. You can specify items related to Namespace access account when Namespace type is set to <code>File system</code> and Content sharing is set to <code>Off</code> .
		User	Displays the user name of the account for viewing the namespace.
		Password	Enter the password of the account for viewing the namespace. The entered password is displayed by using asterisks (*).
		Confirm password	Enter the character string you specified for Password . The entered password is displayed by using asterisks (*).
	Replica system name	Specify the system name of the replica HCP system if replication is used at the location of the HCP system. After changing the system name of the replica HCP, click the Test Connection button to check that the system can be connected to the replica HCP system. You can specify this item when Namespace type is set to <code>File system</code> and Content sharing is set to <code>On (Read-Only)</code> .	
	External Replica HCP host name	When Replica system name is specified, and then the replica HCP system to be linked uses a relaying device, such as a load balancer, when connecting to the network, specify the host name or IP address that has been made external and is used to connect to the replica HCP system.	
Replica namespace FQDN	When Replica system name is specified, the name of the namespace of the replica HCP system is displayed.		
File system settings	Enable the WORM function	Yes or No	Displays whether the WORM function is set for the file system. When linked with an HCP system, the WORM settings items are displayed only if Content sharing is set to <code>Off</code> .
		Auto commit	Switches between displaying or hiding the setting items for autocommit.
		Enable	Yes If this item is selected, autocommit is set for the file system. If this item is not selected, autocommit is not set for the file system.

Item	Description		
			<p>Note that if you enable autocommit, you can no longer disable it.</p> <p>Commit mode</p> <p>Select the mode of autocommit according.</p> <p>Manual</p> <p>Select this to enable autocommit in manual mode.</p> <p>In manual mode, files that are specified as read-only files by clients are subject to the autocommit functionality.</p> <p>Auto</p> <p>Select this to enable autocommit in auto mode.</p> <p>In auto mode, all ordinary files, except for the system files and files in the system directories, are subject to the autocommit functionality.</p> <p>Time until committed</p> <p>If Yes is selected for Enable, specify the time until autocommit is performed. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) spin boxes.</p> <p>After you have specified the setting, you cannot change it.</p> <p>Default retention period</p> <p>Specify the default retention period. Specify a value from 1 minute to 36,500 days in the day(s), hour(s), and minute(s) spin boxes.</p> <p>Select Infinite to set an unlimited default retention period.</p> <p>Enable rename of empty directories</p> <p>Yes</p> <p>Select this to allow renaming of empty directories in a WORM file system.</p>
	Optimize for Large file transfer	Yes	<p>Select this to use the Large File Transfer function.</p> <p>This item is displayed if Content sharing is Off.</p> <p>This item is displayed if the version of linked HCP system is 8.0 or later.</p>

Item	Description	
		<p>Note that the Active File Migration function is automatically enabled when the Large File Transfer function is enabled, even if the Active File Migration function is disabled by using the <code>arcactmigctl</code> command.</p>
	<p>Lower limit of the file size</p>	<p>Specify the lower threshold for the size of files to which the Large File Transfer function is applied. A value in the range from 50 MB to 5 TB can be specified. MB, GB, or TB can be selected as the unit.</p> <p>This item can be specified in cases where Off is selected for Content sharing and Yes is selected for Optimize for Large file transfer.</p> <p>This item is displayed if the version of linked HCP system is 8.0 or later.</p>
<p>Use file version restore</p>	<p>Yes</p>	<p>Select this to make the past version files (past version directories) migrated to the HCP system available to clients. In addition, select how past-version directories are to be kept in the <code>.history</code> directory.</p> <p>You can specify items related to file version restore only if Content sharing is set to a selection other than <code>On (Read-Only)</code>.</p>
	<p>Custom schedule</p>	<p>Select this if you want to use a custom schedule for keeping past-version directories. For details about custom scheduling of the file version restore functionality, see the <i>Installation and Configuration Guide</i>.</p>
	<p>Schedule settings</p>	<p>Configure a custom schedule.</p> <ul style="list-style-type: none"> • Keep 15-MINUTE versions for: The oldest past version directory with 15-minute time units (hour <i>n</i>, minutes 00 to 14, minutes 15 to 29, minutes 30 to 44, minutes 45 to 59) is kept for the number of units specified. Specify any of the following: 15, 30, 45, and 60. • Keep HOURLY versions for: The oldest past version directory with hourly time units (hour <i>n</i>, minutes 00 to 59) is kept for the number of units specified. Specify in the range from 1 to 48. • Keep DAILY versions for: The oldest past version directory with daily time units (day <i>n</i>, 00:00 to

Item	Description		
			<p>23:59) is kept for the number of units specified. Specify in the range from 1 to 62.</p> <ul style="list-style-type: none"> • Keep WEEKLY versions for: The oldest past version directory with weekly time units (week <i>n</i>, Sunday, 00:00 to Saturday, 23:59) is kept for the number of units specified. Specify in the range from 1 to 156. • Keep MONTHLY versions for: The oldest past version directory with monthly time units (month <i>n</i>, 1st day, 00:00 to <i>last-day</i>, 23:59) is kept for the number of units specified. Specify in the range from 1 to 72. • Keep YEARLY versions for: The oldest past version directory with yearly time units (year <i>n</i>, Jan 1, 00:00 to Dec 31, 23:59) is kept for the number of units specified. Specify in the range from 1 to 100.
		Period to hold ^{#2}	Select this if you want to keep past-version directories for each migration interval. Specify a value between 1 and 36,500 for the number of days for which the past-version directories are to be kept.
	CIFS bypass traverse checking	Enable	Select this to enable CIFS bypass traverse checking. This item is not displayed when Content sharing is set to <code>Home directory</code> .
<p>#1: Automatically reconfigures the inode area and moves up to 10 GB of data outside of the inode area if the file system capacity is expanded when all of the following conditions are met:</p> <ul style="list-style-type: none"> - The capacity of the file system after expansion is 1 TB or more. - The file system does not support 64-bit inodes. <p>The system message KAQM04288-I is output when reconfiguration of the inode area starts, and the system message KAQM04289-I is output when reconfiguration is complete.</p> <p>In addition, reconfiguration of the inode area takes up to about 50 minutes to be performed as a background process, with processing affecting the access performance of the system. For this reason, expand the capacity of the file system when the system is accessed less frequently.</p> <p>#2: Note that the retention period of past version directories depends on the capacity of the namespace in the migration destination. For information on how to estimate the</p>			

Item	Description
	capacity requirement for a namespace in a migration destination, see the <i>Installation and Configuration Guide</i> .

Delete File System dialog box

You can delete a file system.

To display the **Delete File System** dialog box, display the **File Systems** window, and then, in the **File Systems** tab, click the line for the file system to be deleted, and then click the **Delete** button.

Table C-165 Items displayed in the Delete File System dialog box

Item		Description
Shares	Share Name	Displays the name of the share.
	Protocol	Displays the names of the protocols used by the file share.
Yes, I have read the above warning and wish to delete the specified file system. check box		Select this check box if you want to delete the file system.
Apply button		Delete the file system. The Yes, I have read the above warning and wish to delete the specified file system. check box must be selected before you click this button.

Advanced ACL Settings dialog box

In the **Advanced ACL Settings** dialog box, you can set ACLs for the shared directory.

To display the **Advanced ACL Settings** dialog box, in the **Create File System** dialog box, click the **Setting** button in **ACL Registered Users and Groups**.

Table C-166 Items displayed in the Advanced ACL Settings dialog box

Item		Description
ACL registered users and groups	User or group name	Specify the name of the target user or group. This is not case sensitive in Windows. You can also specify the following built-in accounts in a Windows domain: <ul style="list-style-type: none"> Everyone Specify this as a group (by clicking the Group Add > button). <ul style="list-style-type: none"> CREATOR GROUP

Item		Description
		<p>Specify this as a group (by clicking the Group Add > button).</p> <ul style="list-style-type: none"> CREATOR OWNER <p>Specify this as a user (by clicking the User Add > button).</p>
	Permissions	<p>Select in the check box whether to allow or deny access. Only operations corresponding to the items for which Allow is selected are allowed.</p> <ul style="list-style-type: none"> Full control Modify Read and execute Read Write List folder contents
	Apply these ACLs to this folder, subfolders, and files	<p>Select this check box to apply the ACL settings to the subfolders and files as well as the selected folder (shared directory). If this check box is not selected, the ACL settings are applied to the selected folder only.</p> <p>We recommend that you do not select this check box when you create an NFS share.</p>
User Add > button		Click this button to add an ACE for the specified user.
Group Add > button		Click this button to add an ACE for the specified group.
< Delete button		Click this button to delete ACEs for users or groups in the ACL Registered Users and Groups area.
ACL Registered Users and Groups area		Displays the ACEs set for the shared directory. For details about the displayed items, see Table C-167 Items displayed in the ACL Registered Users and Groups area in the Advanced ACL Settings dialog box on page C-236 .

Table C-167 Items displayed in the ACL Registered Users and Groups area in the Advanced ACL Settings dialog box

Item	Description
Type	Displays the type of the target user or group. This item is displayed when the ACL type is <code>Advanced ACL</code> .
Name	Displays the name of the target user or group.
Account Type	Displays whether the account has been registered as a user or group.
Permissions	Displays the operation permissions for which access is allowed or denied.

Item	Description
Apply to	Displays whether the ACL settings are applied to the subfolders and files as well as the selected folder (shared directory).

Add Cache Resident Policy dialog box

You can add cache resident policies, which contain conditions for not turning files into stub files when data is migrated to the HCP system.

To display the **Add Cache Resident Policy** dialog box, open the *file-system-name* window, and from the **Cache Resident Policy** tab, click the **Add** button.

Table C-168 Items displayed in the Add Cache Resident Policy dialog box

Item	Description
File system name	Displays the name of the file system to which the policy will be added.
Policy name	Specifies the name of the policy to be added in 32 characters or less. Specify names that have not yet been used in the file system. You can use alphanumeric characters, spaces, and underscores (_).
Directory	Specifies a directory in which you do not want to turn any of the files into stub files.
File types (extensions)	Specifies the extensions of the files that you do not want to turn into stub files. To specify multiple file types, separate each one with a colon (:).
File size range	Specifies the minimum and maximum file sizes in the range from 1 KB to 1,024 TB in which you do not want to turn files into stub files. Specify an integer file size, and then select a unit (KB , MB , GB or TB) from the drop-down list. If you do not want to set a file size range, specify N/A . For the maximum file size, specify a file size greater than the minimum file size or specify N/A .
Comments	Specifies comments about the policy.

Edit Cache Resident Policy dialog box

You can edit cache resident policies, which contain conditions for not turning files into stub files when data is migrated to the HCP system.

To display the **Edit Cache Resident Policy** dialog box, open the *file-system-name* window, and then, in the **Cache Resident Policy** tab, click the line that contains the policy you want to edit, and then click the **Edit** button.

Table C-169 Items displayed in the Edit Cache Resident Policy dialog box

Item	Description
File system name	Displays the name of the file system to which the policy to be edited belongs.
Policy name	Displays the name of the policy to be edited. The policy name cannot be changed.
Directory	Specifies a directory in which you do not want to turn any of the files into stub files.
File types (extensions)	Specifies the extensions of the files that you do not want to turn into stub files. To specify multiple file types, separate each one with a colon (:).
File size range	Specifies the minimum and maximum file sizes in the range from 1 KB to 1,024 TB in which you do not want to turn files into stub files. Specify an integer file size, and then select a unit (KB , MB , GB or TB) from the drop-down list. If you do not want to set a file size range, specify N/A . For the maximum file size, specify a file size greater than the minimum file size or specify N/A .
Comments	Specifies comments about the policy.

Delete Cache Resident Policy dialog box

You can delete cache resident policies, which contain conditions for not turning files into stub files when data is migrated to the HCP system.

To display the **Delete Cache Resident Policy** dialog box, open the *file-system-name* window, and then, in the **Cache Resident Policy** tab, click the line that contains the policy you want to delete, and then click the **Delete** button.

Table C-170 Items displayed in the Delete Cache Resident Policy dialog box

Item		Description
Policy	Policy name	Displays the name of the policy to be deleted.
	Comments	Displays comments about the policy.
Apply button		Click this button to delete the policy.

Provisioning Wizard

You can link to the HCP Anywhere to automatically configure the system and services.

To automatically display **Provisioning Wizard**, change the password for the system administrator account in the **Change System Admin Password** dialog box.

Table C-171 Pages displayed in the Provisioning Wizard

Pages	Description
1. Introduction	<p>Check the contents displayed on the page, and then click Next.</p> <p>To manually configure the system or services, click the Manual Settings button. When the Manual Settings button is clicked, a confirmation dialog box appears, and then System Configuration Wizard appears. After you select to manually configure the system or services, Provisioning Wizard can no longer be used even if you cancel System Configuration Wizard.</p>
2. Provisioning Settings	<p>Specify the following information, and then click Next.</p> <ul style="list-style-type: none"> • The URL for accessing the HCP Anywhere • The password for accessing the HCP Anywhere • Serial number (in case of VMware Appliance) • Setting the proxy server (optional): host name, port number, user name and password used for authentication on the proxy server <p>If the network information for connecting to the HCP Anywhere is not set on the node, click the Setup Network button, and then set the node network information. For details about System Configuration Wizard, see System Configuration Wizard on page C-23.</p>
3. Execution	<p>Displays the progress of system and service configuration based on the information acquired from the HCP Anywhere.</p>
4. Completion	<p>Make sure that the processing results are correct, and then click Close.</p>



Operation performed by end users

The end users registered by the local authentication, the NIS server, or the LDAP server (used for user authentication) can use the GUI to view information such as information about file shares and quota information and change the logon password. This appendix explains how to use the GUI as an end-user.

- [List of operations](#)
- [Logging on](#)
- [Basic GUI operations](#)
- [GUI reference](#)

List of operations

As an end user, you can perform the following tasks:

- View a list of NFS file shares (see [List of File Shares page \(for List of NFS file shares\) on page D-3](#)).
- View a list of CIFS file shares (see [List of File Shares page \(for List of CIFS File Shares\) on page D-4](#)).
- View quota information set for a user (see [Display Quota page \(for User Quota Info.\) on page D-4](#)).
- View quota information set for a group (see [Display Quota page \(for Group Quota Info.\) on page D-6](#)).
- Change your log on password (see [Password Setup page on page D-8](#)).
- View and edit a user comment (see [User Info. Setup page on page D-8](#)).

Logging on

You can open the log on window by specifying the following URL in the web browser.

`https://node-IP-address-or-host-name/index.cgi`

Specify the ID and password, and then click **Login**. The **List of File Shares** page (for List of NFS File Shares) is shown.

To log off, click **Close**. The log off operations will not be performed when you directly quit your web browser.

Basic GUI operations

This section describes the basic operations of the GUI used by end users.

GUI layout

The following figure shows the layout of the GUI used by end users.

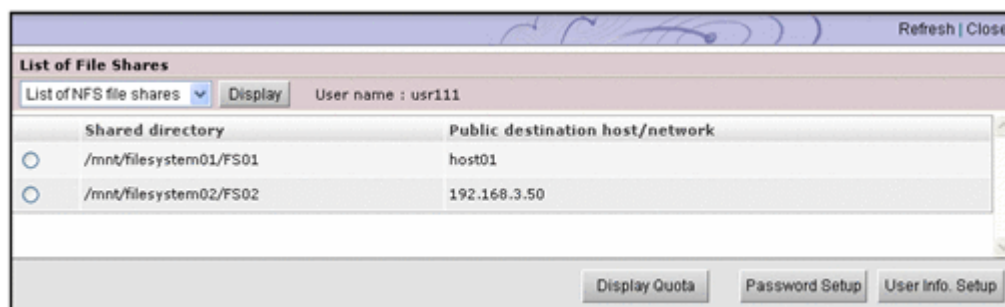


Figure D-1 GUI layout (for end users)

The following explains the components common to all pages.

Refresh

Click to refresh the information displayed in a page used to view a list or status. Although **Refresh** also appears in other pages, clicking **Refresh** in such pages does not refresh any information.

Close

Click to close the current window.

User name

Name of the logged-on user.

Notes about using the GUI

Note the following points when you use the GUI:

- You will be forced to log off if you do not access the program for 30 minutes or more during your log on session.
- When using a wheel mouse, do not rotate the wheel while pressing the **Shift** key. This operation might cause the page to change to another and the running operation to end abnormally. If an error occurs when using the wheel mouse and the **Shift** key, you must log off by clicking **Close**, and then log on again.

If **Close** is not displayed, click the **X** on the title bar to close the window, and then log on again.

- Do not use the Web browser menu (or shortcuts) to perform any operations other than the following:
 - Change text size
 - Copy
 - Paste

Performing an operation other than those noted above might affect the behavior of the GUI.

GUI reference

This section describes the GUI windows used by end users.

List of File Shares page (for List of NFS file shares)

In the **List of File Shares** page (for `List of NFS File Shares`), an end user can view a list of NFS shares.

You can view the **List of File Shares** page (for `List of NFS File Shares`) by selecting **List of NFS file shares** in the drop-down list and then clicking **Display** in the **List of File Shares** page.

The following table lists the information shown in the **List of File Shares** page (for `List of NFS File Shares`).

Table D-1 Information displayed in the List of File Shares page (for List of NFS File Shares)

Item	Description
Shared directory	Name of a shared directory
Public destination host/ network	Public destination host or network

List of File Shares page (for List of CIFS File Shares)

In the **List of File Shares** page (for List of CIFS File Shares), an end user can view a list of CIFS shares.

You can view the **List of File Shares** page (for List of CIFS File Shares) by selecting **List of CIFS file shares** from the drop-down list and then clicking **Display** in the **List of File Shares** page.

The following table lists the information shown in the **List of File Shares** page (for List of CIFS File Shares).

Table D-2 Information displayed in the List of File Shares page (for List of CIFS File Shares)

Item	Description
Name of file share	Name of a CIFS share
Shared directory	Name of a shared directory
Comment for file share	Comment for the CIFS share

Display Quota page (for User Quota Info.)

In the **Display Quota** page (for User Quota Info.), end users can view their own quota information set for each file system.

You can view the **Display Quota** page (for User Quota Info.) by selecting a shared directory or share name and then clicking **Display Quota** in the **List of File Shares** page (for List of NFS File Shares or List of CIFS File Shares).

The following table lists the user quota information shown in the **Display Quota** page (for User Quota Info.).

Table D-3 User quota information displayed in the Display Quota page (for User Quota Info.)

Item	Description
Name of file share or Shared directory	For a CIFS share, Name of file share displays the name of the CIFS share whose quota information is being viewed.

Item	Description
	For an NFS share, Shared directory displays the name of the shared directory whose quota information is being viewed.
Current used block capacity	Amount of block space being used by each user (units: MB) Shown in red if the amount exceeds the value set as the soft limit or reaches the hard limit. The displayed value is rounded up to the nearest ones place. If there is less than 1 MB left before the amount reaches the Hard limit of block , it might not be possible to create a new file.
Soft limit of block	Soft limit (warning value) for block usage
Hard limit of block	Hard limit (upper bound) for block usage
Block grace period	Remaining grace time until new blocks can no longer be assigned after the block usage exceeds the soft limit. Displayed in one of the following formats: <i>n days</i> The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining. <i>n hours</i> The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains. Over The grace time has elapsed. Shown in red. - The block usage is less than the soft limit.
Current used i-node count	Usage of inode for each user Shown in red if it exceeds the value set as the soft limit or reaches the hard limit.
Soft limit of i-node	Soft limit (warning value) for inode usage
Hard limit of i-node	Hard limit (upper bound) for inode usage
i-node grace period	Remaining grace time until files can no longer be created after the inode usage exceeds the soft limit. Displayed in one of the following formats: <i>n days</i> The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining. <i>n hours</i> The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains. Over

Item	Description
	The grace time has elapsed. Shown in red.
	-
	The user's inode usage is less than the soft limit.

Display Quota page (for Group Quota Info.)

In the **Display Quota** page (for *Group Quota Info.*), end users can view the quota information set for each file system for the group to which they belong.

You can view the **Display Quota** page (for *Group Quota Info.*) by selecting **Group quota info.** from the drop-down list and then clicking **Display** in the **Display Quota** page (for *User Quota Info.*).

The following table lists the group quota information displayed in the **Display Quota** page (for *Group Quota Info.*).

Table D-4 Group quota information displayed in the Display Quota page (for Group Quota Info.)

Item	Description
Name of file share or Shared directory	For a CIFS share, Name of file share displays the name of the CIFS share whose quota information is being viewed. For an NFS share, Shared directory displays the name of the shared directory whose quota information is being viewed.
Group name	Name of a group to which the logged-on user belongs
Block	Availability of the block for each group Used capacity Amount of block space being used Shown in red if the amount exceeds the value set as the soft limit or reaches the hard limit. The displayed value is rounded up to the nearest ones place. If there is less than 1 MB left before the amount reaches the Hard limit , it might not be possible to create a new file. Soft limit Soft limit (warning value) for block usage Hard limit Hard limit (upper bound) for block usage Grace period Remaining grace time until new blocks can no longer be assigned after the block usage exceeds the soft limit. Displayed in one of the following forms:

Item	Description
	<p><i>n</i> days The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining.</p> <p><i>n</i> hours The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains.</p> <p>Over The grace time has elapsed. Shown in red.</p> <p>- The block usage is less than the soft limit.</p>
i-node	<p>Availability of inodes for each group</p> <p>Used count Usage of inode Shown in red if it exceeds the value set as the soft limit or reaches the hard limit.</p> <p>Soft limit Soft limit (warning value) for inode usage by the group</p> <p>Hard limit Hard limit (upper bound) for inode usage by the group</p> <p>Grace period Remaining grace time until files can no longer be created after the inode usage exceeds the soft limit. Displayed in one of the following forms:</p> <p><i>n</i> days The remaining grace time is 24 hours or longer. For example, <i>1 days</i> appears if there are 24 hours or more, but less than 48 hours remaining.</p> <p><i>n</i> hours The remaining grace time is less than 24 hours. The value is shown in orange. For example, <i>0 hours</i> appears if less than 1 hour remains.</p> <p>Over The grace time has elapsed. Shown in red.</p> <p>- The block usage is less than the soft limit.</p>
Block grace period	Block grace period set for the file system to which the shared directory belongs
i-node grace period	inode grace period set for the file system to which the shared directory belongs

Password Setup page

From the **Password Setup** page, end-users registered by using local authentication can change their logon passwords. We advise end-users to regularly change their passwords.

If user information has been registered in the CIFS environment, the change is also applied to the password for CIFS user authentication.

You can view the **Password Setup** page by clicking the **Password Setup** button in the **List of File Shares** page (for `List of NFS File Shares` or `List of CIFS File Shares`).

The following table lists the information to be specified in the **Password Setup** page.

Table D-5 Information specified in the Password Setup page

Item	Description
Current password	Enter your current password.
New password	Enter your new password, using from 6 to 20 characters. You can use alphanumeric characters and the following symbols: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~
Re-enter new password	Re-enter the new password that you specified in New password .

User Info. Setup page

In the **User Info. Setup** page, end-users who are logged on and have been registered by using local authentication can edit the comments in their user information.

You can view the **User Info. Setup** page by clicking the **User Info. Setup** button in the **List of File Shares** page (for `List of NFS File Shares` or `List of CIFS File Shares`).

The following table lists the information displayed in the **User Info. Setup** page.

Table D-6 Information displayed in the User Info. Setup page

Item	Description
User name	User name
UID	User ID
Comment	Comment for the user If you want to change the comment, enter a maximum of 32 characters. You can use alphanumeric characters and the following symbols:

Item	Description
	# % & ' () * + - . / ; < > ? @ [] ^ _ { } ~ You can also specify spaces, but spaces cannot be specified at the beginning nor at the end of the character string. If you leave this item blank, no comment is entered.



Reserved words

This appendix lists the words reserved by the system.

- [List of reserved words](#)

List of reserved words

The words reserved for the host name of a node are shown in the following table.

Table E-1 List of reserved words for the host name of a node

Category	Reserved words
A	add, admin
C	CLU_partition, cluster
D	Data_management, debian, define, delete
F	Failover_policy, Filesystem, for, force
H	ha_parameter, ha_services, hostname
I	in, IP_address
L	localhost, log_group, LVM_volume
M	maintenance_off, maintenance_on, modify, move
N	NFS, NFS_admin, node
O	offline, online
R	remove, resource, resource_group, resource_type, RUS_management
S	set, show, start, status, stop, SyncImage
T	to
V	Vserver
Symbol	One period (.), two periods (..)

Note: The reserved words in the above table cannot be specified for the host name of a node regardless of case.

The words reserved for the user name are shown in the following table.

Table E-2 List of reserved words for the user name

Category	Reserved words
A	avahi, avahi-autoipd
B	backup, bin, bind
D	daemon, Debian-exim
E	enasroot
F	ftp
G	games, gdm, gnats
H	haldaemon, hddsroot, hplip, hsguiroot
I	identd, irc

Category	Reserved words
L	libuuid, libvirt-qemu, list, lp
M	mail, man, messagebus
N	nasroot, news, nobody, ntp
O	offline, online
P	postgres, proftpd, proxy
R	root
S	service, snmp, sshd, statd, sync, sys
T	telnetd
U	uucp
V	vde2-net
W	www-data
Symbol	__groupowner

The word reserved for the group name are shown in the following table.

Table E-3 List of reserved words for the group name

Category	Reserved words
A	adm, audio, avahi, avahi-autoipd
B	backup, bin, bind
C	cdrom, crontab
D	daemon, Debian-exim, dialout, dip, disk
E	enasroot
F	fax, floppy, ftp
G	games, gdm, gnats
H	haldaemon, hddsroot, hsguiroot
I	irc
K	kmem, kvm
L	libuuid, libvirt, list, lp, lpadmin
M	mail, man, messagebus, mlocate
N	nasroot, netdev, news, nogroup, ntp
O	operator
P	plugdev, postgres, powerdev, proxy
R	root

Category	Reserved words
S	sasl, scanner, service, shadow, src, ssh, ssl-cert, staff, stb-admin, sudo, sys
T	tape, telnetd, tty
U	users, utmp, uucp
V	vde2-net, video, voice
W	winbindd_priv, www-data

MIB objects

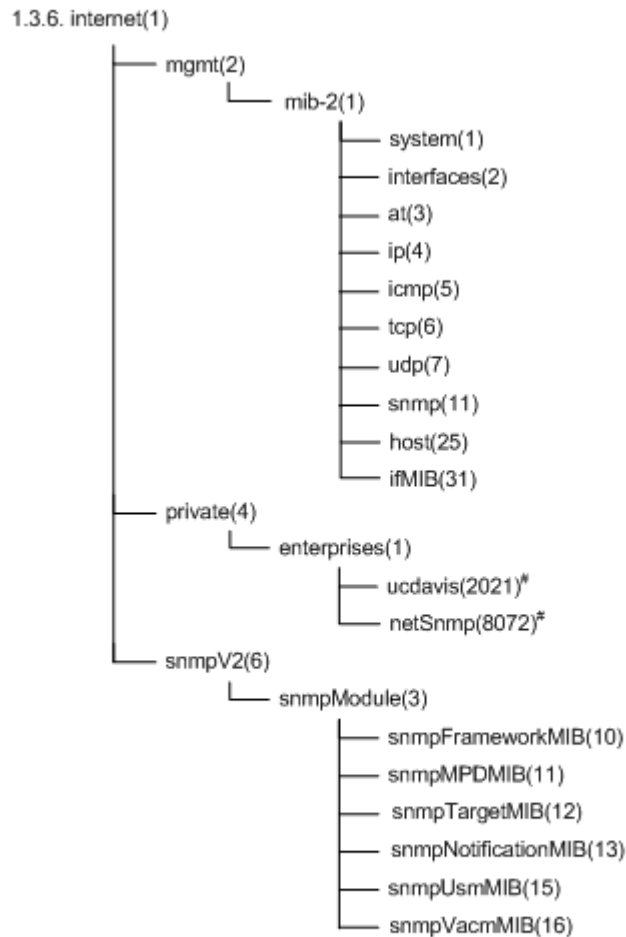
This appendix explains SNMP MIB objects used in the HDI system.

- [List of MIB objects](#)
- [MIB objects for responding to SNMP get requests](#)
- [MIB objects used for SNMP traps](#)

List of MIB objects

This appendix explains MIB objects that are used to respond to SNMP `get` requests in the HDI system, and MIB objects that are used for SNMP traps in the HDI system.

The following figures describe the structures for standard MIB objects and Hitachi's unique Management Information Base (MIB) objects used in the HDI system:



#: Since the MIB objects in `ucdavis(2021)` and `netSnmp(8072)` for `private(4)` group are functionality provided by the SNMP agent package, they are treated as standard MIB objects.

Figure F-1 Structure for standard MIB objects

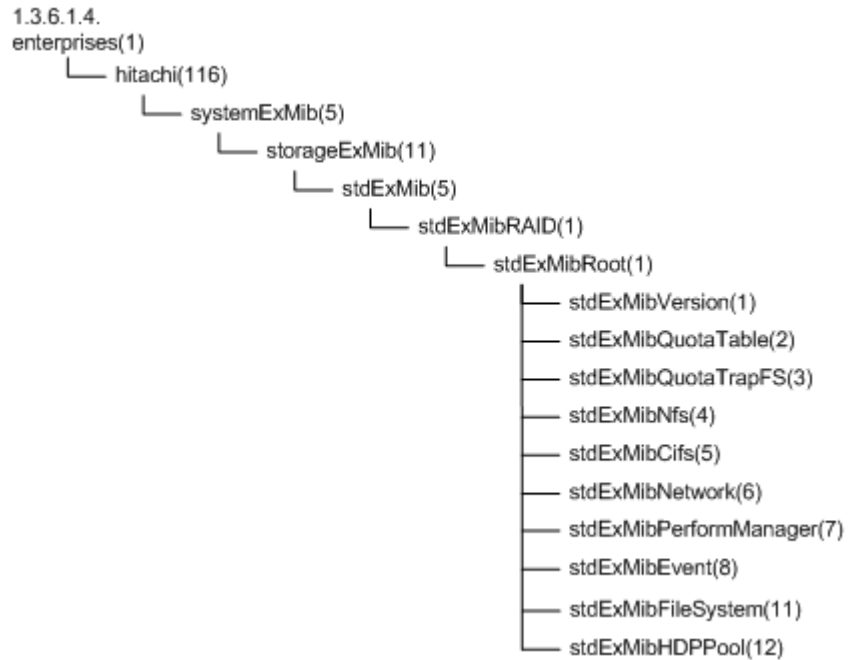


Figure F-2 Groups of MIB objects for responding to SNMP get requests and tables to be referenced (standard MIB objects)

MIB objects for responding to SNMP get requests

The following describes MIB objects used to send responses to SNMP get requests.

The typical MIB objects

The following shows the typical MIB objects used to send responses to SNMP get requests.

Information about CPUs and processes

ucdavis (2021) group

Memory usage

ucdavis (2021) group

Information about networks and interfaces

ifMIB (31) group, stdExMibPerformManager (7) group

Information about file systems

stdExMibQuotaTable (2) group, stdExMibFileSystem (11) group

Table F-1 MIB objects for CPUs

OID	Object name	Description
.1.3.6.1.4.1.2021.10.1.3	laLoad	The load average value, expressed as a string.

OID	Object name	Description
		laLoad-1 stores the accumulated value for the last minute. laLoad-2 stores the accumulated value for the last 5 minutes. laLoad-3 stores the accumulated value for the last 15 minutes.
.1.3.6.1.4.1.2021.11.9	ssCpuUser	The ratio of CPU capacity used by the user.
.1.3.6.1.4.1.2021.11.10	ssCpuSystem	The ratio of CPU capacity used by the system.
.1.3.6.1.4.1.2021.11.11	ssCpuIdle	The ratio of CPU capacity that is idle.
.1.3.6.1.4.1.2021.11.50	ssCpuRawUser	The time for which the user is using the CPU.
.1.3.6.1.4.1.2021.11.52	ssCpuRawSystem	The time for which the system is using the CPU.
.1.3.6.1.4.1.2021.11.53	ssCpuRawIdle	The time for which the CPU is idle.
.1.3.6.1.4.1.2021.11.54	ssCpuRawWait	CPU time spent waiting for I/O.

Table F-2 MIB objects for memory devices

OID	Object name	Description
.1.3.6.1.4.1.2021.4.4	memAvailSwap	The amount of unused swap file space.
.1.3.6.1.4.1.2021.4.6	memAvailReal	The amount of real memory available.
.1.3.6.1.4.1.2021.4.14	memBuffer	The total amount of buffer memory.
.1.3.6.1.4.1.2021.4.15	memCached	The total amount of cache memory.

Table F-3 MIB objects for networks

OID	Object name	Description
.1.3.6.1.2.1.31.1.1.1.6	ifHCInOctets	The total number of octets received on the interface.
.1.3.6.1.2.1.31.1.1.1.10	ifHCOctets	The total number of octets transmitted out of the interface.
.1.3.6.1.4.1.116.5.11.5.1.1.7.1.1.4	nwpmCollision	The number of collisions.
.1.3.6.1.4.1.116.5.11.5.1.1.7.1.1.5	nwpmBuffErrRcvPacket	The number of received packets that were discarded because of buffer insufficiency.

Table F-4 MIB objects related to the file system

OID	Object name	Description
.1.3.6.1.4.1.116.5.11.5.1.1.2.1.6.1.13	quotaUser64UsedCount	The number of blocks used (KB)
.1.3.6.1.4.1.116.5.11.5.1.1.2.1.6.1.16	quotaUser64FileCount	The number of inodes used
.1.3.6.1.4.1.116.5.11.5.1.1.2.1.7.1.13	quotaGroup64UsedCount	The used capacity of the subtree quota (for 64bit) (KB)
.1.3.6.1.4.1.116.5.11.5.1.1.2.1.7.1.16	quotaGroup64FileCount	The number of inodes used
.1.3.6.1.4.1.116.5.11.5.1.1.11.1.1.8	fileSystemKBUsed	File system block usage (KB)
.1.3.6.1.4.1.116.5.11.5.1.1.11.1.1.11	fileSystemUsedPercent	File system usage rate (%)
.1.3.6.1.4.1.116.5.11.5.1.1.11.1.1.12	fileSystemKBAvail	File system unused capacity (KB)
.1.3.6.1.4.1.116.5.11.5.1.1.11.1.1.15	fileSystemInodeUsed	Number of used inodes
.1.3.6.1.4.1.116.5.11.5.1.1.11.1.1.16	fileSystemInodeFree	Number of unused inodes

List of MIB object

The following table lists the environments in which the MIB objects that are used to respond to SNMP `get` requests can be obtained and the tables to be referenced.

Table F-5 Environments in which the MIB objects used to respond to SNMP `get` requests can be obtained and the tables to be referenced (standard MIB objects)

Group name		Definition RFC number	Description	Tables
1.3.6.1.2.mib-2 (1)	system (1)	1907	This group is for system information.	Table F-7 system (1) group on page F-8
	interfaces (2)	1213	This group is for interfaces information.	Table F-8 interfaces (2) group on page F-8
	at (3)	1213	This group is for at information.	Table F-9 at (3) group on page F-10

Group name		Definition RFC number	Description	Tables
	ip (4)	1213	This group is for <code>ip</code> information.	Table F-10 ip (4) group on page F-10
	icmp (5)	1213	This group is for <code>icmp</code> information.	Table F-11 icmp (5) group on page F-18
	tcp (6)	1213	This group is for <code>tcp</code> information.	Table F-12 tcp (6) group on page F-19
	udp (7)	1213	This group is for <code>udp</code> information.	Table F-13 udp (7) group on page F-21
	snmp (11)	1907	This group is for <code>snmp</code> information.	Table F-14 snmp (11) group on page F-22
	host (25)	2790	This group is for <code>host</code> information.	Table F-15 host (25) group on page F-24
	ifMIB (31)	2233	This group is for <code>ifMIB</code> information.	Table F-16 ifMIB (31) group on page F-29
	ipv6MIB (55)	2465	This group is for <code>ipv6MIB</code> information.	Table F-17 ipv6MIB (55) group on page F-31
1.3.6.1.4.enterprises (1)	ucdavis (2021)	N/A	This group is for <code>ucdavis</code> information.	Table F-18 ucdavis (2021) group on page F-32
	netSnmp (8072)	N/A	This group is for <code>netSnmp</code> information.	Table F-19 netSnmp (8072) group on page F-39
1.3.6.1.6.snmpModules (3)	snmpFrameworkMIB (10)	2271	This group is for <code>snmp</code> management structures.	Table F-20 snmpFrameworkMIB (10) group on page F-42
	snmpMPDMIB (11)	2272	This group is for message processing.	Table F-21 snmpMPDMIB (11) group on page F-42
	snmpTargetMIB (12)	2273	This group is for parameter formation, for message creation.	Table F-22 snmpTargetMIB (12) group on page F-43

Group name		Definition RFC number	Description	Tables
	snmpNotificationMIB (13)	2273	This group is for parameter formation, for notification.	Table F-23 snmpNotificationMIB (13) group on page F-44
	snmpUsmMIB (15)	2274	This group is for security information definition.	Table F-24 snmpUsmMIB (15) group on page F-45
	snmpVacmMIB (16)	2275	This group is for access/control information definition.	Table F-25 snmpVacmMIB (16) group on page F-46
Note: N/A = Not applicable.				

Table F-6 Environments in which the MIB objects used to respond to SNMP get requests can be obtained and the tables to be referenced (Hitachi MIB objects)

Group name	Description	Tables
stdExMibVersion (1)	This group is for version information.	Not applicable
stdExMibQuotaTable (2)	This group is for quota management.	Table F-26 stdExMibQuotaTable (2) group on page F-48
stdExMibNfs (4)	This group is for NFS.	Table F-27 stdExMibNfs (4) group on page F-55
stdExMibCifs (5)	This group is for CIFS.	Table F-28 stdExMibCifs (5) group on page F-63
stdExMibNetwork (6)	This group is for the network.	Table F-29 stdExMibNetwork (6) group on page F-63
stdExMibPerformManager (7)	This group is for performance management.	Table F-30 stdExMibPerformManager (7) group on page F-64
stdExMibFileSystem (11)	This group is for file systems.	Table F-31 stdExMibFileSystem (11) group on page F-65
stdExMibHDPPool (12)	This group is for pools.	Table F-32 stdExMibHDPPool (12) group on page F-67

Tables [Table F-7 system \(1\) group on page F-8](#) to [Table F-32 stdExMibHDPPool \(12\) group on page F-67](#) summarize the groups of MIB objects used in responding to SNMP `get` requests. In the tables, the type is described as - for the MIB objects that have no data types and have `Entry` types (which are in table structure and therefore cannot be accessed).

Table F-7 system (1) group

ID	Object name	Type	Meaning
1	sysDescr (1)	DisplayString	Names or version numbers for the hardware, OS, and network OS.
2	sysObjectID (2)	OBJECT IDENTIFIER	Vendor authentication ID for the network management subsystem.
3	sysUpTime (3)	TimeTicks	Time elapsed since system startup.
4	sysContact (4)	DisplayString	Contact information for the management node.
5	sysName (5)	DisplayString	The name and domain name of the management node.
6	sysLocation (6)	DisplayString	Location in which the management node is set up.
7	sysServices (7)	INTEGER	A value indicating services.
8	sysORLastChange (8)	TimeTicks	The latest value for <code>sysUpTime</code> .
9	sysORTable (9)	-	For each MIB module, lists the functions of the local SNMPv2 entity acting as an agent.
9.1	sysOREntry (1)	-	Contains <code>sysORTable</code> entries.
9.1.1	sysORIndex (1)	INTEGER	A support variable used to identify instances of <code>sysORTable</code> columns and objects. This cannot be obtained.
9.1.2	sysORID (2)	OBJECT IDENTIFIER	Indicates proper identifiers for each MIB module. MIB modules are supported based on the local SNMPv2 entity acting as an agent.
9.1.3	sysORDescr (3)	DisplayString	Defines a text description of the function identified by the corresponding <code>sysORID</code> .
9.1.4	sysORUpTime (4)	TimeStamp	Indicates the value of <code>sysUpTime</code> at the time this overview row was last instantiated.

Table F-8 interfaces (2) group

ID	Object name	Type	Meaning
1	ifNumber (1)	Integer32	The number of network interfaces provided by the system
2	ifTable (2)	-	The interface entity table
2.1	ifEntry (1)	-	A list of interface information belonging to the sub-network layer
2.1.1	ifIndex (1)	InterfaceIndex	A number identifying this interface (values are sequential, from 1 to <code>ifNumber</code>)

ID	Object name	Type	Meaning
2.1.2	ifDescr (2)	DisplayString	Information about the interface
2.1.3	ifType (3)	IANAifType	The interface type
2.1.4	ifMtu (4)	Integer32	The maximum size of datagrams that can be transmitted with this interface
2.1.5	ifSpeed (5)	Gauge32	An estimate of the current line speed for this interface ^{#1}
2.1.6	ifPhysAddress (6)	PhysAddress	The physical address immediately below the network layer of this interface
2.1.7	ifAdminStatus (7)	INTEGER	The desired status for this interface Each value represents the following: 1: up, 2: down, 3: testing
2.1.8	ifOperStatus (8)	INTEGER	The current status of this interface Each value represents the following: 1: up, 2: down, 3: testing, 4: unknown, 5: dormant, 6: notPresent, 7: lowerLayerDown
2.1.9	ifLastChange (9)	TimeTicks	The value of <code>sysUpTime</code> at the time at which <code>ifOperStatus</code> was last changed for this interface
2.1.10	ifInOctets (10)	Counter32	The number of octets received with this interface ^{#2}
2.1.11	ifInUcastPkts (11)	Counter32	The number of unicast packets for which the upper protocol has been notified ^{#3}
2.1.12	ifInNUcastPkts (12)	Counter32	The number of non-unicast packets (broadcast or multicast packets) for which the upper protocol has been notified
2.1.13	ifInDiscards (13)	Counter32	The number of packets for which no errors occurred, but nevertheless could not be passed to the upper protocol (the number of incoming packets that were discarded, with no buffer, etc.)
2.1.14	ifInErrors (14)	Counter32	The number of packets that could not be received because an error occurred within the packet
2.1.15	ifInUnknownProtos (15)	Counter32	The number of packets discarded, because of receiving unsupported protocol
2.1.16	ifOutOctets (16)	Counter32	The number of octets from packets transmitted with this interface ^{#2}
2.1.17	ifOutUcastPkts (17)	Counter32	The number of unicast packets sent by the upper layer ^{#3}
2.1.18	ifOutNUcastPkts (18)	Counter32	The number of non-unicast packets sent by the upper layer

ID	Object name	Type	Meaning
2.1.19	ifOutDiscards (19)	Counter32	The number of packets with no errors, but that were discarded during transmission processing (for which the transmission buffer was insufficient, and so on.)
2.1.20	ifOutErrors (20)	Counter32	The number of packets that could not be sent because of an error
2.1.21	ifOutQLen (21)	Gauge32	The size of the queue for transmission packets
2.1.22	ifSpecific (22)	OBJECT IDENTIFIER	A reference to a MIB defining properties of the interface media The object ID of a MIB is dependent on <code>ifType</code>
<p>#1: The estimated line speed for a GbE interface is 100,000,000 bps. This is the value output by standard MIBs for GbE interfaces. The estimated line speed for 10 GbE and trunking-port interfaces is not close to the actual value. The advertised speed of a 10 GbE port is 10,000,000,000 bps, but the estimated value is always set to 4,294,967,295. The estimated value for a trunking port is always set to 100,000,000.</p> <p>#2: <code>ifInOctets</code> and <code>ifOutOctets</code> are 32-bit counters, and are reset if there is 100 Mbps of traffic within 5 minutes.</p> <p>#3: <code>ifInUcastPkts</code> and <code>ifOutUcastPkts</code> are 32-bit counters, and might be reset if the system is continuously run for a long time.</p>			

Table F-9 at (3) group

ID	Object name	Type	Meaning
1	atTable (1)	-	The table for <code>NetworkAddress</code> for the corresponding value of the physical address
1.1	atEntry (1)	-	A list related to one <code>NetworkAddress</code> for the corresponding value of the physical address for each entry
1.1.1	atIfIndex (1)	INTEGER	The value of <code>ifIndex</code> for the corresponding interface
1.1.2	atPhysAddress (2)	PhysAddress	The physical address
1.1.3	atNetAddress (3)	NetworkAddresses	The IP address corresponding to <code>atPhysAddress</code> , depending on the media

Table F-10 ip (4) group

ID	Object name	Type	Meaning
1	ipForwarding (1)	INTEGER	Availability of IP relay functionality (whether or not operation is performed by gateway) Each value represents the following: 1: forwarding, 2: notForwarding
2	ipDefaultTTL (2)	Integer32	The default TTL setting in IP headers

ID	Object name	Type	Meaning
3	ipInReceives (3)	Counter32	The total number of IP datagrams received from all interfaces
4	ipInHdrErrors (4)	Counter32	The number of datagrams received and then discarded because of IP header errors
5	ipInAddrErrors (5)	Counter32	The number of packets discarded because of an invalid destination address in the IP header
6	ipForwDatagrams (6)	Counter32	The number of packets for which relay was deemed necessary
7	ipInUnknownProtos (7)	Counter32	The number of IP data programs discarded because of the following: <ul style="list-style-type: none"> The protocol cannot be confirmed for incoming IP packets. The protocol is unsupported.
8	ipInDiscards (8)	Counter32	The total number of IP datagrams discarded during transmission for reasons other than errors
9	ipInDelivers (9)	Counter32	The number of IP datagrams reported to the upper layer
10	ipOutRequests (10)	Counter32	The total number of IP datagrams requested by the upper layer, for IP packet transmission
11	ipOutDiscards (11)	Counter32	The number of IP datagrams discarded for reasons other than errors
12	ipOutNoRoutes (12)	Counter32	The number of IP datagrams discarded because no transmission route was specified
13	ipReasmTimeout (13)	Integer32	The maximum number of seconds to hold fragment packets waiting for reassembly
14	ipReasmReqds (14)	Counter32	The number of incoming IP datagrams for which reassembly is necessary
15	ipReasmOKs (15)	Counter32	The number of incoming IP datagrams for which reassembly was successful
16	ipReasmFails (16)	Counter32	The number of incoming IP datagrams for which reassembly failed
17	ipFragOKs (17)	Counter32	The number of IP datagrams for which fragmentation was successful
18	ipFragFails (18)	Counter32	The number of IP datagrams for which fragmentation failed
19	ipFragCreates (19)	Counter32	The number of IP datagram fragments created as a result of fragmentation
20	ipAddrTable (20)	-	A table for addressing information related to the IP address of this entity

ID	Object name	Type	Meaning
			(a table of address information by IP address)
20.1	ipAddrEntry (1)	-	A list of addressing information for one of the IP addresses of this entity
20.1.1	ipAdEntAddr (1)	IpAddress	IP address
20.1.2	ipAdEntIfIndex (2)	INTEGER	The index value for the interface used by this entry
20.1.3	ipAdEntNetMask (3)	IpAddress	The subnet mask for the IP address of this entry
20.1.4	ipAdEntBcastAddr (4)	INTEGER	The value of the lowest bit of the address during IP broadcast transmission
20.1.5	ipAdEntReasmMaxSize (5)	INTEGER	The maximum IP packet size that can be reassembled from input IP datagrams that were divided into IP fragments received by the interface [#]
21	ipRouteTable (21)	-	The IP routing table for this entity
21.1	ipRouteEntry (1)	-	Routing information for a specified destination
21.1.1	ipRouteDest (1)	IpAddress	The destination IP address of this route
21.1.2	ipRouteIfIndex (2)	INTEGER	The index value of the interface existing on the first hop of this route
21.1.3	ipRouteMetric1 (3)	INTEGER	The primary routing metric of this route
21.1.4	ipRouteMetric2 (4)	INTEGER	The alternate routing metric of this route [#]
21.1.5	ipRouteMetric3 (5)	INTEGER	The alternate routing metric of this route [#]
21.1.6	ipRouteMetric4 (6)	INTEGER	The alternate routing metric of this route [#]
21.1.7	ipRouteNextHop (7)	IpAddress	The IP address of the next hop of this route
21.1.8	ipRouteType (8)	INTEGER	The route type Each value represents the following: 1: other, 2: invalid, 3: direct, 4: indirect
21.1.9	ipRouteProto (9)	INTEGER	The routing structure that learned the route Each value represents the following: 1: other, 2: local, 3: netmgmt, 4: icmp, 5: egp, 6: ggp, 7: hello, 8: rip, 9: is-is, 10: es-is, 11: ciscoIgrp, 12: bbnSpfIgp, 13: ospf, 14: gbp

ID	Object name	Type	Meaning
21.1.10	ipRouteAge (10)	INTEGER	The amount of time elapsed since the route was updated [#]
21.1.11	ipRouteMask (11)	IpAddress	The subnet mask value for ipRouteDest
21.1.12	ipRouteMetric5 (12)	INTEGER	The alternate routing metric of this route [#]
21.1.13	ipRouteInfo (13)	OBJECT IDENTIFIER	A reference to the MIB object defining the specific routing protocol that can be trusted on this route
22	ipNetToMediaTable (22)	-	The IP address conversion table used to map a physical address from IP addresses
22.1	ipNetToMediaEntry (1)	-	A list of individual IP addresses that correspond to the physical address
22.1.1	ipNetToMediaIfIndex (1)	INTEGER	The ID number of the active interface
22.1.2	ipNetToMediaPhysAddress (2)	PhysAddress	The media-dependent physical address
22.1.3	ipNetToMediaNetAddress (3)	IpAddress	The IP address corresponding to the media-dependent physical address
22.1.4	ipNetToMediaType (4)	INTEGER	The mapping type Each value represents the following: 1: other, 2: invalid, 3: dynamic, 4: static
23	ipRoutingDiscards (23)	Counter	The number of routing entries selected for rejection despite being active, such as those rejected because of an insufficient buffer for the routing table
24	ipForward (24)	-	The MIB module for the management of CIDR multipath IP Routes
24.4	ipCidrRouteTable (4)	-	The IP CIDR entity's IP Routing table
24.4.1	ipCidrRouteEntry (1)	-	An ipCidrRoute entry
24.4.1.1	ipCidrRouteDest (1)	IpAddress	The destination IP address
24.4.1.2	ipCidrRouteMask (2)	IpAddress	The IP address and the mask value
24.4.1.3	ipCidrRouteTos (3)	Integer32	The IP TOS Field
24.4.1.4	ipCidrRouteNextHop (4)	IpAddress	On remote routes, the address of the next system en route
24.4.1.5	ipCidrRouteIfIndex (5)	Integer32	The index value of the local interface
24.4.1.6	ipCidrRouteType (6)	INTEGER	The type of route Each value represents the following: 1: other, 2: reject, 3: local, 4: remote

ID	Object name	Type	Meaning
24.4.1.7	ipCidrRouteProto (7)	INTEGER	The routing mechanism via which this route was learned Each value represents the following: 1: other, 2: local, 3: netmgmt, 4: icmp, 5: egg, 6: ggp, 7: hello, 8: rip, 9: isIs, 10: esIs, 11: ciscoIgrp, 12: bbnSpfIgp, 13: ospf, 14: bgp, 15: idpr, 16: ciscoEigrp
24.4.1.9	ipCidrRouteInfo (9)	OBJECT IDENTIFIER	A reference to MIB definitions specific to the particular routing protocol that is responsible for this route
24.4.1.10	ipCidrRouteNextHopAS (10)	Integer32	The Autonomous System Number of the Next Hop
24.4.1.11	ipCidrRouteMetric1 (11)	Integer32	The primary routing metric
24.4.1.12	ipCidrRouteMetric2 (12)	Integer32	An alternate routing metric
24.4.1.13	ipCidrRouteMetric3 (13)	Integer32	An alternate routing metric
24.4.1.14	ipCidrRouteMetric4 (14)	Integer32	An alternate routing metric
24.4.1.15	ipCidrRouteMetric5 (15)	Integer32	An alternate routing metric
24.4.1.16	ipCidrRouteStatus (16)	RowStatus	The row status variable Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
24.6	inetCidrRouteNumber (6)	Gauge32	The number of inetCidrRouteTable entries
24.7	inetCidrRouteTable (7)	-	The inet CIDR table
24.7.1	inetCidrRouteEntry (1)	-	An inetCidrRoute entry
24.7.1.7	inetCidrRouteIfIndex (7)	InterfaceIndexOrZero	The index value that identifies the local interface
24.7.1.8	inetCidrRouteType (8)	INTEGER	The type of route Each value represents the following: 1: other, 2: reject, 3: local, 4: remote, 5: blackhole
24.7.1.9	inetCidrRouteProto (9)	IANAipRouteProtocol	The routing mechanism via which this route was learned Each value represents the following: 1: other, 2: local, 3: netmgmt, 4: icmp, 5: egg, 6: ggp, 7: hello, 8: rip,

ID	Object name	Type	Meaning
			9: isIs, 10: esIs, 11: ciscoIgrp, 12: bbnSpfIgp, 13: ospf, 14: bgp, 15: idpr, 16: ciscoEigrp, 17: dvmrp
24.7.1.1.10	inetCidrRouteAge (10)	Gauge32	The number of seconds since this route was last updated
24.7.1.1.11	inetCidrRouteNextHopAS (11)	InetAutonomousSystemNumber	The Autonomous System Number of the Next Hop
24.7.1.1.12	inetCidrRouteMetric1 (12)	Integer32	The primary routing metric
24.7.1.1.13	inetCidrRouteMetric2 (13)	Integer32	An alternate routing metric
24.7.1.1.14	inetCidrRouteMetric3 (14)	Integer32	An alternate routing metric
24.7.1.1.15	inetCidrRouteMetric4 (15)	Integer32	An alternate routing metric
24.7.1.1.16	inetCidrRouteMetric5 (16)	Integer32	An alternate routing metric
24.7.1.1.17	inetCidrRouteStatus (17)	RowStatus	The row status variable Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
25	ipv6IpForwarding (25)	INTEGER	The indication of whether this entity is acting as an IPv6 router on any interface in respect to the forwarding of datagrams received by, but not addressed to, this entity Each value represents the following: 1: forwarding, 2: notForwarding
26	ipv6IpDefaultHopLimit (26)	Unsigned32	The default value inserted into the Hop Limit field of the IPv6 header
31	ipTrafficStats (31)	-	The received traffic statistics
31.1	ipSystemStatsTable (1)	-	The ipSystemStats table
31.1.1	ipSystemStatsEntry (1)	-	An ipSystemStats entry
31.1.1.3	ipSystemStatsInReceives (3)	Counter32	The total number of datagrams received
31.1.1.4	ipSystemStatsHCInReceives (4)	Counter64	The total number of datagrams received
31.1.1.5	ipSystemStatsInOctets (5)	Counter32	The total number of octets received

ID	Object name	Type	Meaning
31.1.1.6	ipSystemStatsHCInOctets (6)	Counter64	The total number of octets received
31.1.1.7	ipSystemStatsInHdrErrors (7)	Counter32	The number of datagrams discarded because of errors in their IP headers
31.1.1.9	ipSystemStatsInAddrErrors (9)	Counter32	The number of datagrams discarded because the IP address in their IP header's destination field was not a valid address
31.1.1.10	ipSystemStatsInUnknownProtos (10)	Counter32	The number of datagrams received successfully but discarded because of an unknown or unsupported protocol
31.1.1.12	ipSystemStatsInForwardDatagrams (12)	Counter32	The number of IP datagrams for which this entity was not their final IP destination and for which this entity attempted to find a route to forward them to that final destination
31.1.1.13	ipSystemStatsHCInForwardDatagrams (13)	Counter64	The number of IP datagrams for which this entity was not their final IP destination and for which this entity attempted to find a route to forward them to that final destination
31.1.1.14	ipSystemStatsReasmReqds (14)	Counter32	The number of IP fragments received that needed to be reassembled
31.1.1.15	ipSystemStatsReasmOKs (15)	Counter32	The number of IP datagrams successfully reassembled
31.1.1.16	ipSystemStatsReasmFails (16)	Counter32	The number of failures detected by the IP re-assembly algorithm
31.1.1.17	ipSystemStatsInDiscards (17)	Counter32	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but were discarded
31.1.1.18	ipSystemStatsInDelivers (18)	Counter32	The total number of IP datagrams successfully delivered
31.1.1.20	ipSystemStatsOutRequests (20)	Counter32	The total number of IP datagrams transmitted
31.1.1.21	ipSystemStatsHCOutRequests (21)	Counter64	The total number of IP datagrams transmitted
31.1.1.22	ipSystemStatsOutNoRoutes (22)	Counter32	The number of IP datagrams discarded
31.1.1.24	ipSystemStatsHCOutForwardDatagrams (24)	Counter64	The number of datagrams for which this entity was not their final IP destination and for which it was successful in finding a path to their final destination
31.1.1.25	ipSystemStatsOutDiscards (25)	Counter32	The number of output IP datagrams for which no problem was encountered to

ID	Object name	Type	Meaning
			prevent their transmission to their destination, but were discarded
31.1.1.28	ipSystemStatsOutFragFails (28)	Counter32	The number of IP datagrams that have been discarded because they needed to be fragmented but could not be
31.1.1.29	ipSystemStatsOutFragCreates (29)	Counter32	The number of output datagram fragments that have been generated
31.1.1.46	ipSystemStatsDiscontinuityTime (46)	TimeStamp	The time on the most recent occasion at which any one or more of this entry's counters suffered a discontinuity
31.1.1.47	ipSystemStatsRefreshRate (47)	Unsigned32	The minimum reasonable polling interval
34	ipAddressTable (34)	-	The ipAddress table
34.1	ipAddressEntry (1)	-	An ipAddress entry
34.1.1	ipAddressIfIndex (1)	InterfaceIndex	The index
34.1.4	ipAddressType (4)	INTEGER	The type of address Each value represents the following: 1: unicast, 2: anycast, 3: broadcast
34.1.5	ipAddressPrefix (5)	RowPointer	A pointer to the row in the prefix table
34.1.6	ipAddressOrigin (6)	IpAddressOriginTC	The origin of the address Each value represents the following: 1: other, 2: manual, 4: dhcp, 5: linklayer, 6: random
34.1.7	ipAddressStatus (7)	IpAddressStatusTC	The status of the address Each value represents the following: 1: preferred, 2: deprecated, 3: invalid, 4: inaccessible, 5: unknown, 6: tentative, 7: duplicate, 8: optimistic
34.1.8	ipAddressCreated (8)	TimeStamp	The value of sysUpTime at the time this entry was created
34.1.9	ipAddressLastChanged (9)	TimeStamp	The value of sysUpTime at the time this entry was last updated
34.1.10	ipAddressRowStatus (10)	RowStatus	The status of ipAddress Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
34.1.11	ipAddressStorageType (11)	StorageType	The storage type for ipAddress Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly

ID	Object name	Type	Meaning
35	ipNetToPhysicalTable (35)	-	The ipNetToPhysical table
35.1	ipNetToPhysicalEntry (1)	-	An ipNetToPhysical entry
35.1.4	ipNetToPhysicalPhysAddress (4)	PhysAddress	The MAC address
35.1.6	ipNetToPhysicalType (6)	INTEGER	The type of IP address Each value represents the following: 1: other, 2: invalid, 3: dynamic, 4: static, 5: local
35.1.7	ipNetToPhysicalState (7)	INTEGER	The status of the IP address Each value represents the following: 1: reachable, 2: stale, 3: delay, 4: probe, 5: invalid, 6: unknown, 7: incomplete
35.1.8	ipNetToPhysicalRowStatus (8)	RowStatus	The status of the ipNetToPhysical row Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
#: These cannot be obtained.			

Table F-11 icmp (5) group

ID	Object name	Type	Meaning
1	icmpInMsgs (1)	Counter32	The total number of ICMP messages received by this entity
2	icmpInErrors (2)	Counter32	The number of ICMP error messages received (such as those for checksum errors and frame length errors)
3	icmpInDestUnreachs (3)	Counter32	The number of ICMP Destination Unreachable messages received
4	icmpInTimeExcds (4)	Counter32	The number of ICMP Time Exceed messages received
5	icmpInParmProbs (5)	Counter32	The number of ICMP Parameter Problem messages received
6	icmpInSrcQuenchs (6)	Counter32	The number of ICMP Source Quench messages received
7	icmpInRedirects (7)	Counter32	The number of ICMP Network Redirect messages received
8	icmpInEchos (8)	Counter32	The number of ICMP Echo request messages received

ID	Object name	Type	Meaning
9	icmpInEchoReps (9)	Counter32	The number of ICMP Echo response messages received
10	icmpInTimestamps (10)	Counter32	The number of ICMP TimeStamp request messages received
11	icmpInTimestampReps (11)	Counter32	The number of ICMP TimeStamp response messages received
12	icmpInAddrMasks (12)	Counter32	The number of ICMP Address Mask request messages received
13	icmpInAddrMaskReps (13)	Counter32	The number of incoming ICMP Address Mask response messages
14	icmpOutMsgs (14)	Counter32	The total number of ICMP send attempts (including those for which errors occurred)
15	icmpOutErrors (15)	Counter32	The number of ICMP messages that were not sent because of an error
16	icmpOutDestUnreachs (16)	Counter32	The number of ICMP Destination Unreachable messages sent
17	icmpOutTimeExcds (17)	Counter32	The number of ICMP Time Exceeded messages sent
18	icmpOutParmProbs (18)	Counter32	The number of ICMP Parameter Problem messages sent
19	icmpOutSrcQuenchs (19)	Counter32	The number of ICMP Source Quench messages sent
20	icmpOutRedirects (20)	Counter32	The number of ICMP Redirect messages sent
21	icmpOutEchos (21)	Counter32	The number of ICMP Echo request messages sent
22	icmpOutEchoReps (22)	Counter32	The number of ICMP Echo response messages sent
23	icmpOutTimestamps (23)	Counter32	The number of ICMP Timestamp request messages sent
24	icmpOutTimestampReps (24)	Counter32	The number of ICMP Timestamp response messages sent
25	icmpOutAddrMasks (25)	Counter32	The number of ICMP Address Mask request messages sent
26	icmpOutAddrMaskReps (26)	Counter32	The number of ICMP Address Mask response messages sent

Table F-12 tcp (6) group

ID	Object name	Type	Meaning
1	tcpRtoAlgorithm (1)	INTEGER	The algorithm to decide the timeout time used for retransmission

ID	Object name	Type	Meaning
			Each value represents the following: 1: other, 2: constant, 3: rsre, 4: vanj, 5: rfc2988
2	tcpRtoMin (2)	Integer32	The minimum value for the retransmission timeout time
3	tcpRtoMax (3)	Integer32	The maximum value for the retransmission timeout time
4	tcpMaxConn (4)	Integer32	The total number of supportable TCP connections. -1 is returned when this number is dynamic
5	tcpActiveOpens (5)	Counter32	The number of times that TCP connections were moved from the CLOSE status to the SYN-SENT status
6	tcpPassiveOpens (6)	Counter32	The number of times that TCP connections were moved from the LISTEN status to the SYN-RCVD status
7	tcpAttemptFails (7)	Counter32	The number of times TCP connections were moved from the SYN-SENT or SYN-RCVD statuses to the CLOSE status, and added to the number of times TCP connections were moved from the SYN-RCVD status to the LISTEN status
8	tcpEstabResets (8)	Counter32	The number of times TCP connections were moved from the ESTABLISHED or CLOSE-WAIT statuses to the CLOSE status
9	tcpCurrEstab (9)	Gauge32	The total number of TCP connections in the ESTABLISHED or CLOSE-WAIT status
10	tcpInSegs (10)	Counter32	The total number of incoming segments, including error segments [#]
11	tcpOutSegs (11)	Counter32	The total number of segments sent [#]
12	tcpRetransSegs (12)	Counter32	The total number of resent segments
13	tcpConnTable (13)	-	A table of information specific to TCP connections
13.1	tcpConnEntry (1)	-	Entry information about a particular TCP connection
13.1.1	tcpConnState (1)	INTEGER	The TCP connection status Each value represents the following: 1: closed, 2: listen, 3: synSent, 4: synReceived, 5: established, 6: finWait1, 7: finWait2, 8: closeWait, 9: lastAck, 10: closing, 11: timeWait, 12: deleteTCB
13.1.2	tcpConnLocalAddress (2)	IpAddress	The local IP address of this TCP connection

ID	Object name	Type	Meaning
13.1.3	tcpConnLocalPort (3)	Integer32	The local port number of this TCP connection
13.1.4	tcpConnRemAddress (4)	IpAddress	The remote IP address of this TCP connection
13.1.5	tcpConnRemPort (5)	Integer32	The remote port number of this TCP connection
14	tcpInErrs (14)	Counter32	The total number of error segments received
15	tcpOutRsts (15)	Counter32	The number of segments sent that have the RST flag
19	tcpConnectionTable (19)	-	The TCP connection table
19.1	tcpConnectionEntry (1)	-	A TCP connection entry
19.1.7	tcpConnectionState (7)	INTEGER	The state of the TCP connection for the IP address Each value represents the following: 1: closed, 2: listen, 3: synSent, 4: synReceived, 5: established, 6: finWait1, 7: finWait2, 8: closeWait, 9: lastAck, 10: closing, 11: timeWait, 12: deleteTCB
19.1.8	tcpConnectionProcess (8)	Unsigned32	The process ID for the process connected to the network
#: ifInUcastPkts and ifOutUcastPkts are 32-bit counters, and might be reset if the system is continuously run for a long time.			

Table F-13 udp (7) group

ID	Object name	Type	Meaning
1	udpInDatagrams (1)	Counter32	The number of UDP datagrams reported to the upper layer
2	udpNoPorts (2)	Counter32	The total number of incoming UDP packets for which no parent application exists in the address port
3	udpInErrors (3)	Counter32	The number of UDP datagrams unable to be reported to the application because of reasons other than <code>udpNoPorts</code>
4	udpOutDatagrams (4)	Counter32	The total number of UDP datagrams sent by the parent application
5	udpTable (5)	-	A table for UDP listener information
5.1	udpEntry (1)	-	The number of entries for a particular UDP listener
5.1.1	udpLocalAddress (1)	IpAddress	The local IP address of this UDP listener

ID	Object name	Type	Meaning
5.1.2	udpLocalPort (2)	Integer32	The local port number of this UDP listener
5.7	udpEndpointTable (7)	-	The UDP EndPoint information table
5.7.1	udpEndPointEntry (1)	-	A UDP EndPoint entry
5.7.1.8	udpEndPointProcess (8)	Unsigned32	The process ID for the process associated with the network endpoint

Table F-14 snmp (11) group

ID	Object name	Type	Meaning
1	snmpInPkts (1)	Counter32	The total number of incoming SNMP messages
2	snmpOutPkts (2)	Counter32	The total number of outgoing SNMP messages
3	snmpInBadVersions (3)	Counter32	The total number of incoming messages of unsupported versions
4	snmpInBadCommunityNames (4)	Counter32	The total number of incoming SNMP messages for unused communities
5	snmpInBadCommunityUses (5)	Counter32	The total number of incoming messages indicating operations not allowed by the community
6	snmpInASNParseErrors (6)	Counter32	The total number of incoming ASN.1 error messages
8	snmpInTooBigs (8)	Counter32	The total number of incoming PDUs for which the error status is <code>tooBig</code>
9	snmpInNoSuchNames (9)	Counter32	The total number of incoming PDUs for which the error status is <code>noSuchName</code>
10	snmpInBadValues (10)	Counter32	The total number of incoming PDUs for which the error status is <code>badValue</code>
11	snmpInReadOnlys (11)	Counter32	The total number of incoming PDUs for which the error status is <code>readOnly</code>
12	snmpInGenErrs (12)	Counter32	The total number of incoming PDUs for which the error status is <code>genErr</code>
13	snmpInTotalReqVars (13)	Counter32	The total number of MIB objects for which MIB collection was successful
14	snmpInTotalSetVars (14)	Counter32	The total number of MIB objects for which MIB setup was successful
15	snmpInGetRequests (15)	Counter32	The total number of <code>GetRequestPDUS</code> received
16	snmpInGetNexts (16)	Counter32	The total number of <code>GetNextRequestPDUS</code> received

ID	Object name	Type	Meaning
17	snmpInSetRequests (17)	Counter32	The total number of SetRequestPDUS received
18	snmpInGetResponses (18)	Counter32	The total number of GetResponsePDUS received
19	snmpInTraps (19)	Counter32	The total number of TrapPDUS received
20	snmpOutTooBigs (20)	Counter32	The total number of outgoing PDUs for which the error status is tooBig
21	snmpOutNoSuchNames (21)	Counter32	The total number of outgoing PDUs for which the error status is noSuchName
22	snmpOutBadValues (22)	Counter32	The total number of outgoing PDUs for which the error status is badValue
24	snmpOutGenErrs (24)	Counter32	The total number of outgoing PDUs for which the error status is genErr
25	snmpOutGetRequests (25)	Counter32	The total number of GetRequestPDUS sent
26	snmpOutGetNexts (26)	Counter32	The total number of GetNextRequestPDUS sent
27	snmpOutSetRequests (27)	Counter32	The total number of SetRequestPDUS sent
28	snmpOutGetResponses (28)	Counter32	The total number of GetResponsePDUS sent
29	snmpOutTraps (29)	Counter32	The total number of TrapPDUS sent
30	snmpEnableAuthentTraps (30)	INTEGER	Indicates whether an authentication-failure Trap was issued Each value represents the following: 1: enabled, 2: disabled
31	snmpSilentDrops (31)	Counter32	Indicates the total number, sent to the SNMP entity, of GetRequest-PDUS, GetNextRequest-PDUS, GetBulkRequest-PDUS, SetRequest-PDUS, and InformRequest-PDUS. (If the size of a response containing an alternate Response-PDU with a blank variable binding field is larger than the local limit, or the maximum message size on the side from which the request originated, the snmpSilentDrops object will be discarded without being reported.)
32	snmpProxyDrops (32)	Counter32	Indicates the total number, sent to the SNMP entity, of GetRequest-PDUS, GetNextRequest-PDUS, GetBulkRequest-PDUS, SetRequest-PDUS, and InformRequest-PDUS. (If the transmission of messages (which are probably converted) to the proxy target fails

ID	Object name	Type	Meaning
			without a <code>Response-PDU</code> being returned (aside from timeouts), the <code>snmpProxyDrops</code> object will be discarded without being reported.)
<p>Note: These MIB information items are reset when SNMP agents are restarted. Because SNMP agents are restarted in an HDI system once a day, information for only one day is stored at most.</p>			

Table F-15 host (25) group

ID	Object name	Type	Meaning
1	hrSystem (1)	-	Host resource system
1.1	hrSystemUptime (1)	TimeTicks	Time elapsed since system initialization
1.2	hrSystemDate (2)	DateAndTime	Current date and time
1.3	hrSystemInitialLoad Device (3)	Integer32	The index of the <code>hrDeviceEntry</code> for the device from which this host is configured to load its initial operating system configuration
1.4	hrSystemInitialLoadParameters (4)	International DisplayString	Parameter passed to the kernel after Linux startup
1.5	hrSystemNumUsers (5)	Gauge32	Number of user sessions for which this host is storing state information
1.6	hrSystemProcesses (6)	Gauge32	Number of processes currently loaded
1.7	hrSystemMaxProcesses (7)	Gauge32	Returns the fixed value 0
2	hrStorage (2)	-	System storage area for the host resource
2.1	hrStorageTypes (1)	-	Storage area type for the host resource Note: An OID definition is used as the response for <code>hrStorageType</code> , and this object has no real state. The same is true of objects from OID 2.1.1 to 2.1.10.
2.1.1	hrStorageOther (1)	-	The storage area type for the corresponding index during <code>hrStorageType</code> collection is not OID 2.1.2 to 2.1.10
2.1.2	hrStorageRam (2)	-	The storage area type for the corresponding index during <code>hrStorageType</code> collection corresponds to RAM
2.1.3	hrStorageVirtualMemory (3)	-	The storage area type for the corresponding index during <code>hrStorageType</code> collection corresponds to virtual memory

ID	Object name	Type	Meaning
2.1.4	hrStorageFixedDisk (4)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the hard disk
2.1.5	hrStorageRemovable Disk (5)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the removable disk
2.1.6	hrStorageFloppyDisk (6)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the floppy disk
2.1.7	hrStorageCompactDisc (7)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the compact disc
2.1.8	hrStorageRamDisk (8)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the RAM disk
2.1.9	hrStorageFlashMemory (9)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to the flash memory
2.1.10	hrStorageNetworkDisk (10)	-	The storage area type for the corresponding index during hrStorageType collection corresponds to a file system in the network
2.2	hrMemorySize (2)	KBytes	Amount of main physical memory
2.3	hrStorageTable (3)	-	The (conceptual) table of logical storage area on the host
2.3.1	hrStorageEntry (1)	-	The (conceptual) entry in the logical storage area on the host
2.3.1.1	hrStorageIndex (1)	Integer32	Unique value for each logical storage area for the host
2.3.1.2	hrStorageType (2)	AutonomousType	Storage device type (OID allocated to hrStorageTypes by the index) indicated by this entry
2.3.1.3	hrStorageDescr (3)	DisplayString	Name of the logical storage area
2.3.1.4	hrStorageAllocationUnits (4)	Integer32	Block size allocated from the logical storage area
2.3.1.5	hrStorageSize (5)	Integer32	Block amount
2.3.1.6	hrStorageUsed (6)	Integer32	Block usage
3	hrDevice (3)	-	Device
3.1	hrDeviceTypes (1)	-	Device type

ID	Object name	Type	Meaning
			Note: An OID definition is used as the response for <code>hrDeviceType</code> , and this object has no real state. The same is true of objects from OID 3.1.1 to 3.1.6, or 3.1.10 to 3.1.21.
3.1.1	<code>hrDeviceOther</code> (1)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection is not OID 3.1.2 to 3.1.6, or 3.1.10 to 3.1.21
3.1.2	<code>hrDeviceUnknown</code> (2)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection cannot be recognized
3.1.3	<code>hrDeviceProcessor</code> (3)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the processor (CPU)
3.1.4	<code>hrDeviceNetwork</code> (4)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the network interface
3.1.5	<code>hrDevicePrinter</code> (5)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the printer
3.1.6	<code>hrDeviceDiskStorage</code> (6)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the disk
3.1.10	<code>hrDeviceVideo</code> (10)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the video device
3.1.11	<code>hrDeviceAudio</code> (11)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the audio device
3.1.12	<code>hrDeviceCoprocessor</code> (12)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the coprocessor
3.1.13	<code>hrDeviceKeyboard</code> (13)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the keyboard
3.1.14	<code>hrDeviceModem</code> (14)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the modem
3.1.15	<code>hrDeviceParallelPort</code> (15)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the parallel port
3.1.16	<code>hrDevicePointing</code> (16)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to a pointing device such as a mouse

ID	Object name	Type	Meaning
3.1.17	hrDeviceSerialPort (17)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the serial port
3.1.18	hrDeviceTape (18)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the tape device
3.1.19	hrDeviceClock (19)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to the clock
3.1.20	hrDeviceVolatileMemory (20)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to volatile memory
3.1.21	hrDeviceNonVolatileMemory (21)	-	The device type for the corresponding index during <code>hrDeviceType</code> collection corresponds to non-volatile memory
3.2	hrDeviceTable (2)	-	The (conceptual) table for the devices on the host
3.2.1	hrDeviceEntry (1)	-	The (conceptual) entry for a device on the host
3.2.1.1	hrDeviceIndex (1)	Integer32	Unique value for each device on the host
3.2.1.2	hrDeviceType (2)	AutonomousType	The device type indicated by this entry (OID allocated to <code>hrDeviceTypes</code> by the index)
3.2.1.3	hrDeviceDescr (3)	DisplayString	Device name
3.2.1.4	hrDeviceID (4)	ProductID	Device ID
3.3	hrProcessorTable (3)	-	The (conceptual) table for the processors on the host
3.3.1	hrProcessorEntry (1)	-	The (conceptual) entry for a processor on the host
3.3.1.1	hrProcessorFrwID (1)	ProductID	Processor firmware ID
3.4	hrNetworkTable (4)	-	The (conceptual) table for the network devices on the host
3.4.1	hrNetworkEntry (1)	-	The (conceptual) entry for a network device on the host
3.4.1.1	hrNetworkIfIndex (1)	InterfaceIndexOrZero	Value of <code>ifIndex</code> corresponding to this network device
3.6	hrDiskStorageTable (6)	-	The (conceptual) table for long-term storage devices on the host
3.6.1	hrDiskStorageEntry (1)	-	The (conceptual) entry for a long-term storage device on the host
3.6.1.1	hrDiskStorageAccess (1)	INTEGER	Access attribute Each value represents the following:

ID	Object name	Type	Meaning
			1: readWrite, 2: readOnly
3.6.1.2	hrDiskStorageMedia (2)	INTEGER	Media type Each value represents the following: 1: other, 2: unknown, 3: hardDisk, 4: floppyDisk, 5: opticalDiskROM, 6: opticalDiskWORM, 7: opticalDiskRM, 8: ramDisk
3.6.1.3	hrDiskStorageRemovable (3)	TruthValue	Removability Each value represents the following: 1: true, 2: false
3.6.1.4	hrDiskStorageCapacity (4)	KBytes	Total capacity
3.7	hrPartitionTable (7)	-	The (conceptual) table for long-term storage device partitions on the host
3.7.1	hrPartitionEntry (1)	-	The (conceptual) entry for a long-term storage device partition on the host
3.7.1.1	hrPartitionIndex (1)	Integer32	Unique value for each long-term storage device partition on the host ^{#1}
3.7.1.2	hrPartitionLabel (2)	International DisplayString	Device partition name ^{#1}
3.7.1.3	hrPartitionID (3)	OCTET STRING	Device partition number ^{#1}
3.7.1.4	hrPartitionSize (4)	KBytes	Device partition size ^{#1}
3.7.1.5	hrPartitionFSIndex (5)	Integer32	Index for the device partition file system ^{#1}
3.8	hrFSTabl (8)	-	The (conceptual) table for the file system
3.8.1	hrFSEntry (1)	-	The (conceptual) entry in the file system
3.8.1.1	hrFSIndex (1)	Integer32	Unique value for each file system
3.8.1.2	hrFSMountPoint (2)	International DisplayString	Root path name for this file system
3.8.1.3	hrFSRemoteMountPoint (3)	International DisplayString	Name and address of the server on which this file system is mounted ^{#2}
3.8.1.4	hrFSType (4)	AutonomousType	OID allocated to hrFSTypes by the mount type
3.8.1.5	hrFSAccess (5)	INTEGER	Access attribute Each value represents the following: 1: readWrite, 2: readOnly
3.8.1.6	hrFSBootable (6)	TruthValue	Flag indicating whether the file system can be booted Each value represents the following: 1: true, 2: false

ID	Object name	Type	Meaning
3.8.1.7	hrFSStorageIndex (7)	Integer32	Index to <code>hrStorageEntry</code> indicating information about this file system
3.8.1.8	hrFSLastFullBackupDate (8)	DateAndTime	Last date on which this file system was copied to another storage device for backup ^{#3}
3.8.1.9	hrFSLastPartialBackupDate (9)	DateAndTime	Last date on which part of this file system was copied to another storage device for backup ^{#3}
3.9	hrFSTypes (9)	-	Device type Note: An OID definition is used as the response for <code>hrFSType</code> , and this object has no real state. The same is true of object OID3.9.1.
3.9.1	hrFSOther (1)	-	Only XFS can be used as the file system for this system. Because there are no objects corresponding to XFS in <code>hrFSTypes</code> (8), this object is allocated.
5	hrSWRunPerf (5)	-	Performance table for running software
5.1	hrSWRunPerfTable (1)	-	The (conceptual) table for performance metrics of running software
5.1.1	hrSWRunPerfEntry (1)	-	The (conceptual) entry for performance metrics of running software
5.1.1.1	hrSWRunPerfCPU (1)	Integer32	CPU time spent running a process (units: 10ms)
5.1.1.2	hrSWRunPerfMem (2)	KBytes	Total actual system memory allocated to running processes
<p>#1: These cannot be obtained. #2: Null ("") is always obtained. #3: The value of 0-1-1,0:0:0.0 is always obtained.</p>			

Table F-16 ifMIB (31) group

ID	Object name	Type	Meaning
1	ifMIBObjects (1)	-	The additional object for interface entries
1.1	ifXTable (1)	-	A list of interface entries. The number of entries is given by the value of <code>ifNumber</code> . This table contains additional objects for the interface table
1.1.1	ifXEntry (1)	-	An entry containing additional management information applicable to a particular interface
1.1.1.1	ifName (1)	DisplayString	The textual name of the interface

ID	Object name	Type	Meaning
1.1.1.2	ifInMulticastPkts (2)	Counter32	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer
1.1.1.3	ifInBroadcastPkts (3)	Counter32	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer
1.1.1.4	ifOutMulticastPkts (4)	Counter32	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer
1.1.1.5	ifOutBroadcastPkts (5)	Counter32	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer
1.1.1.6	ifHCInOctets (6)	Counter64	The total number of octets received on the interface. This object is a 64-bit version of ifInOctets
1.1.1.7	ifHCInUcastPkts (7)	Counter64	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts.
1.1.1.8	ifHCInMulticastPkts (8)	Counter64	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. This object is a 64-bit version of ifInMulticastPkts.
1.1.1.9	ifHCInBroadcastPkts (9)	Counter64	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts.
1.1.1.10	ifHCOctets (10)	Counter64	The total number of octets transmitted out of the interface. This object is a 64-bit version of ifOutOctets.
1.1.1.11	ifHCOOutUcastPkts (11)	Counter64	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifOutUcastPkts.
1.1.1.12	ifHCOOutMulticastPkts (12)	Counter64	The total number of packets that higher-level protocols requested be

ID	Object name	Type	Meaning
			transmitted, and which were addressed to a multicast address at this sub-layer. This object is a 64-bit version of ifOutMulticastPkts.
1.1.1.13	ifHCOutBroadcastPkts (13)	Counter64	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifOutBroadcastPkts.
1.1.1.14	ifLinkUpDownTrapEnable (14)	INTEGER	Indicates whether linkUp/linkDown traps should be generated for this interface. Each value represents the following: 1: enabled, 2: disabled
1.1.1.15	ifHighSpeed (15)	Gauge32	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of 'n' then the speed of the interface is somewhere in the range of 'n-500,000' to 'n+499,999'.
1.1.1.16	ifPromiscuousMode (16)	TruthValue	This object has a value of false(2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of true(1) when the station accepts all packets/frames transmitted on the media. Each value represents the following: 1: true, 2: false
1.1.1.17	ifConnectorPresent (17)	TruthValue	This object has the value 'true(1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise. Each value represents the following: 1: true, 2: false
1.1.1.18	ifAlias (18)	DisplayString	This object is an 'alias' name for the interface as specified by a network manager.
1.1.1.19	ifCounterDiscontinuityTime (19)	TimeStamp	The value of sysUpTime on the most recent occasion at which any one or more of this interface's counters suffered a discontinuity

Table F-17 ipv6MIB (55) group

ID	Object name	Type	Meaning
1	ipv6MIBObjects (1)	-	IPv6 MIB objects

ID	Object name	Type	Meaning
1.1	ipv6Forwarding (1)	INTEGER	The indication of whether this entity is acting as an IPv6 router in respect to the forwarding of datagrams received by, but not addressed to, this entity Each value represents the following: 1: forwarding, 2: notForwarding
1.2	ipv6DefaultHopLimit (2)	INTEGER	The default value inserted into the Hop Limit field of the IPv6 header
1.3	ipv6Interfaces (3)	Unsigned32	The number of IPv6 interfaces
1.5	ipv6IfTable (5)	-	The IPv6 Interfaces table contains information on the entity's internetwork-layer interfaces
1.5.1	ipv6IfEntry (1)	-	An interface entry containing objects about a particular IPv6 interface
1.5.1.2	ipv6IfDescr (2)	DisplayString	A textual string containing information about the interface
1.5.1.3	ipv6IfLowerLayer (3)	VariablePointer	The object ID ($\{0,0\}$) that identifies the protocol layer over which this network interface operates
1.5.1.4	ipv6IfEffectiveMtu (4)	Unsigned32	The size of the largest IPv6 packet which can be sent/received on the interface
1.5.1.8	ipv6IfPhysicalAddresses (8)	PhysAddress	The interface's physical address
1.5.1.9	ipv6IfAdminStatus (9)	INTEGER	The desired state of the interface Each value represents the following: 1: up, 2: down
1.5.1.10	ipv6IfOperStatus (10)	INTEGER	The current operational state of the interface Each value represents the following: 1: up, 2: down, 3: noIfIdentifier, 4: unknown, 5: notPresent

Table F-18 ucdavis (2021) group

ID	Object name	Type	Meaning
2	prTable (2)	-	Contains the process status.
2.1	prEntry (1)	-	A hierarchical tree comprising a table that contains a list of process information.
2.1.1	prIndex (1)	Integer32	An index number allocated to this process information.
2.1.2	prNames (2)	DisplayString	The process names specified in that of the <code>proc</code> line.

ID	Object name	Type	Meaning
2.1.3	prMin (3)	Integer32	The minimum value set for the <code>proc</code> line.
2.1.4	prMax (4)	Integer32	The maximum value set for the <code>proc</code> line.
2.1.5	prCount (5)	Integer32	The number of processes specified in <code>prNames</code> that are currently running.
2.1.100	prErrorFlag (100)	UCDErrorFlag	In the case of an error, this is 1. Otherwise, it is 0. Each value represents the following: 0: no error, 1: error
2.1.101	prErrMsg (101)	DisplayString	This contains an error message, when <code>prErrorFlag</code> is 1.
2.1.102	prErrFix (102)	UCDErrorFix	When the administrator sets this object to 1, the command already specified on the <code>procfix</code> line of the <code>snmpd.conf</code> file is run. Each value represents the following: 0: noError, 1: runFix
2.1.103	prErrFixCmd (103)	DisplayString	The name of the command run when <code>prErrFix</code> is set to 1.
4	memory (4)	-	Contains the memory status.
4.1	memIndex (1)	Integer32	A dummy index number (always 0).
4.2	memErrorName (2)	DisplayString	A dummy name (always <code>swap</code>).
4.3	memTotalSwap (3)	Integer32	The amount of space reserved for the swap file.
4.4	memAvailSwap (4)	Integer32	The amount of unused swap file space.
4.5	memTotalReal (5)	Integer32	The amount of real memory installed.
4.6	memAvailReal (6)	Integer32	The amount of real memory available. Note: Nodes use most of the memory as an I/O buffer cache to enable cached I/O data to be reused. For this reason, the amount of memory that is used increases periodically, and the variations in the amount of available memory become smaller.
4.7	memTotalSwapTXT (7)	-	The swap file reserved area that is used for text. ^{#1}
4.8	memAvailSwapTXT (8)	-	The amount of swap file space for text that is unused. ^{#1}
4.9	memTotalRealTXT (9)	-	The total real memory used for text. ^{#1}

ID	Object name	Type	Meaning
4.10	memAvailRealTXT (10)	-	The amount of available memory used for text. ^{#1}
4.11	memTotalFree (11)	Integer32	The total available memory.
4.12	memMinimumSwap (12)	Integer32	The available size of the swap file during an error.
4.13	memShared (13)	Integer32	The total amount of shared memory.
4.14	memBuffer (14)	Integer32	The total amount of buffer memory.
4.15	memCached (15)	Integer32	The total amount of cache memory.
4.100	memSwapError (100)	UCDErrorFlag	The swap error flag. Each value represents the following: 0: noError, 1: runFix
4.101	memSwapErrorMsg (101)	DisplayString	The error message when <code>memSwapError</code> is 1.
8	extTable (8)	-	Runs the commands already specified on the system, and contains the results.
8.1	extEntry (1)	-	A hierarchical tree that holds a table containing data from execution results.
8.1.1	extIndex (1)	Integer32	An index number.
8.1.2	extNames (2)	DisplayString	The name specified for the set name in the <code>exec</code> line.
8.1.3	extCommand (3)	DisplayString	The full path name and arguments of the execution file specified in the <code>exec</code> line.
8.1.100	extResult (100)	Integer32	The error code returned when the execution file specified in <code>extCommand</code> is run.
8.1.101	extOutput (101)	DisplayString	The execution results of the execution file specified in <code>extCommand</code> .
8.1.102	extErrFix (102)	UCDErrorFix	When the administrator sets this object to 1, the command already specified in the <code>execfix</code> line of the <code>snmpd.conf</code> file is run. Each value represents the following: 0: noError, 1: runFix
8.1.103	extErrFixCmd (103)	DisplayString	The name of the command run when <code>extErrFix</code> is set to 1.
9	dskTable (9)	-	Contains the disk status.
9.1	dskEntry (1)	-	A hierarchical tree to hold disk information.
9.1.1	dskIndex (1)	Integer32	An index number.
9.1.2	dskPath (2)	DisplayString	The path name of the inspection target.

ID	Object name	Type	Meaning
			The value specified for the path name to be inspected, in the <code>disk</code> line.
9.1.3	dskDevice (3)	DisplayString	The device name contained in <code>dskPath</code> .
9.1.4	dskMinimum (4)	Integer32	The minimum amount for error handling specified in the <code>disk</code> line (-1 when a percentage is specified).
9.1.5	dskMinPercent (5)	Integer32	The minimum percentage amount for error handling specified in the <code>disk</code> line (-1 when units are specified in KB).
9.1.6	dskTotal (6)	Integer32	The maximum amount that can be stored on the device specified in <code>dskDevice</code> .
9.1.7	dskAvail (7)	Integer32	The amount of space currently available on the device specified in <code>dskDevice</code> .
9.1.8	dskUsed (8)	Integer32	The current usage rate of the device specified in <code>dskDevice</code> .
9.1.9	dskPercent (9)	Integer32	The current usage rate of the device specified in <code>dskDevice</code> , expressed as a percentage.
9.1.10	dskPercentNode (10)	Integer32	The current inode usage rate of the device specified in <code>dskDevice</code> , expressed as a percentage.
9.1.11	dskTotalLow (11)	Unsigned32	Total size of the disk/partition (KB). Together with <code>dskTotalHigh</code> composes 64-bit number. ^{#2} (That is, the two <code>dskTotalHigh</code> and <code>dskTotalLow</code> values require a total of 64 bits.)
9.1.12	dskTotalHigh (12)	Unsigned32	Total size of the disk/partition (KB). Together with <code>dskTotalLow</code> composes 64-bit number. ^{#2} (That is, the two <code>dskTotalHigh</code> and <code>dskTotalLow</code> values require a total of 64 bits.)
9.1.13	dskAvailLow (13)	Unsigned32	Unused capacity on the disk (KB). Together with <code>dskAvailHigh</code> composes 64-bit number. ^{#2} (That is, the two <code>dskAvailHigh</code> and <code>dskAvailLow</code> values require a total of 64 bits.)
9.1.14	dskAvailHigh (14)	Unsigned32	Unused capacity on the disk (KB). Together with <code>dskAvailLow</code> composes 64-bit number. ^{#2} (That is, the two <code>dskAvailHigh</code> and <code>dskAvailLow</code> values require a total of 64 bits.)
9.1.15	dskUsedLow (15)	Unsigned32	Used capacity on the disk (KB). Together with <code>dskUsedHigh</code> composes 64-bit number. ^{#2} (That is, the two <code>dskUsedHigh</code> and <code>dskUsedLow</code> values require a total of 64 bits.)

ID	Object name	Type	Meaning
9.1.16	dskUsedHigh (16)	Unsigned32	Used capacity on the disk (KB). Together with dskUsedLow composes 64-bit number. ^{#2} (That is, the two dskUsedHigh and dskUsedLow values require a total of 64 bits.)
9.1.100	dskErrorFlag (100)	UCDErrorFix	An error flag that indicates whether or not the available space is less than that specified on the <code>disk</code> line. 1: less than or equal to the specified space 0: greater than or equal to the specified space Each value represents the following: 0: noError, 1: runFix
9.1.101	dskErrorMsg (101)	DisplayString	The error message when <code>dskErrorFlag</code> is 1.
10	laTable (10)	-	Contains load average information for the system.
10.1	laEntry (1)	-	A hierarchical directory that contains load average information.
10.1.1	laIndex (1)	Integer32	An index number. This value is 1 for 1 minute average value information, 2 for 5 minute average value information, and 3 for 15 minute average value information.
10.1.2	laNames (2)	DisplayString	The monitoring name. This value is <code>Load-1</code> for 1 minute average value information, <code>Load-5</code> for 5 minute average value information, and <code>Load-15</code> for 15 minute average value information.
10.1.3	laLoad (3)	DisplayString	The load average value, expressed as a string. <code>laLoad-1</code> stores the accumulated value for the last minute. <code>laLoad-2</code> stores the accumulated value for the last 5 minutes. <code>laLoad-3</code> stores the accumulated value for the last 15 minutes.
10.1.4	laConfig (4)	DisplayString	The average value set in the <code>load</code> line for error handling.
10.1.5	laLoadInt (5)	Integer32	<code>laLoad</code> , expressed as a percentage.
10.1.6	laLoadFloat (6)	Float	<code>laLoad</code> , expressed as a floating-point decimal.
10.1.100	laErrorFlag (100)	UCDErrorFix	An error flag.

ID	Object name	Type	Meaning
			This value is 1 when the set average value of the load average is exceeded, and 0 otherwise. Each value represents the following: 0: noError, 1: runFix
10.1.101	laErrorMessage (101)	DisplayString	The error message when laLoadErrorFlag is 1.
11	systemStats (11)	-	Contains the system status.
11.1	ssIndex (1)	Integer32	A dummy index number (always 1).
11.2	ssErrorName (2)	DisplayString	The systemStats name (always systemStats).
11.3	ssSwapIn (3)	Integer32	The time required for swap-in.
11.4	ssSwapOut (4)	Integer32	The time required for swap-out.
11.5	ssIOSent (5)	Integer32	The time required for transmission to the block device.
11.6	ssIOReceive (6)	Integer32	The time required for reception from the block device.
11.7	ssSysInterrupts (7)	Integer32	The number of interruptions for 1 second, including clock interruptions.
11.8	ssSysContext (8)	Integer32	The number of context switches switched for 1 second.
11.9	ssCpuUser (9)	Integer32	The ratio of CPU capacity used by the user.
11.10	ssCpuSystem (10)	Integer32	The ratio of CPU capacity used by the system.
11.11	ssCpuIdle (11)	Integer32	The ratio of CPU capacity that is idle.
11.50	ssCpuRawUser (50)	Counter32	The time for which the user is using the CPU.
11.51	ssCpuRawNice (51)	Counter32	The value of the nice process.
11.52	ssCpuRawSystem (52)	Counter32	The time for which the system is using the CPU.
11.53	ssCpuRawIdle (53)	Counter32	The time for which the CPU is idle.
11.54	ssCpuRawWait (54)	Counter32	CPU time spent waiting for I/O
11.55	ssCpuRawKernel (55)	Counter32	Kernel CPU time
11.56	ssCpuRawInterrupt (56)	Counter32	Interrupt level CPU time
11.57	ssIORawSent (57)	Counter32	Number of requests sent to block devices
11.58	ssIORawReceived (58)	Counter32	Number of requests received from block devices

ID	Object name	Type	Meaning
11.59	ssRawInterrupts (59)	Counter32	Number of interrupts
11.60	ssRawContexts (60)	Counter32	Number of context switches
11.61	ssCpuRawSoftIRQ (61)	Counter32	Time for performing soft interrupt processing
11.62	ssRawSwapIn (62)	Counter32	Number of blocks swapped in
11.63	ssRawSwapOut (63)	Counter32	Number of blocks swapped out
13	ucdExperimental (13)	-	An experimental MIB
13.14	ucdDlmodMIB (14)	-	The dynamic load module MIB. The function for loading a predefined MIB definition file during snmpd operation.
13.14.1	dlmodNextIndex (1)	Integer32	The index of the next-loaded MIB.
13.15	ucdDiskIOMIB (15)	-	This MIB module defines objects for disk I/O statistics.
13.15.1	diskIOTable (1)	-	Table of IO devices and how much data they have read/written
13.15.1.1	diskIOEntry (1)	-	An entry containing a device and its statistics
13.15.1.1.1	diskIOIndex (1)	Integer32	Reference index for each observed device
13.15.1.1.2	diskIODevice (2)	DisplayString	The name of the device we are counting/checking (Example: ram0, sda)
13.15.1.1.3	diskIONRead (3)	Counter32	The number of bytes read from this device since boot (32-bit counter)
13.15.1.1.4	diskIONWritten (4)	Counter32	The number of bytes written to this device since boot (32-bit counter)
13.15.1.1.5	diskIOReads (5)	Counter32	The number of read accesses from this device since boot
13.15.1.1.6	diskIOWrites (6)	Counter32	The number of write accesses to this device since boot
13.15.1.1.12	diskIONReadX (12)	Counter64	The number of bytes read from this device since boot (64-bit version)
13.15.1.1.13	diskIONWrittenX (13)	Counter64	The number of bytes written to this device since boot (64-bit version)
16	logMatch (16)	-	Log search
16.1	logMatchMaxEntries (1)	Integer32	Maximum number of supportable logMatch entries
100	version (100)	-	Contains the snmpd version information.
100.1	versionIndex (1)	Integer32	The index to MIB.

ID	Object name	Type	Meaning
100.2	versionTag (2)	DisplayString	The CVS tag keyword.
100.3	versionDate (3)	DisplayString	The date from the RCS keyword.
100.4	versionCDate (4)	DisplayString	The date from <code>ctime()</code> .
100.5	versionIdent (5)	DisplayString	The ID from the RCS keyword.
100.6	versionConfigureOptions (6)	DisplayString	If this agent is configured, options are moved to the config script.
100.10	versionClearCache (10)	Integer32	When this is set to 1, the execution cache is cleared.
100.11	versionUpdateConfig (11)	Integer32	When this is set to 1, the config file is read.
100.12	versionRestartAgent (12)	Integer32	When this is set to 1, the agent is restarted.
100.13	versionSavePersistentData (13)	Integer32	When this is set to 1, persistent data for the agent is saved immediately.
100.20	versionDoDebugging (20)	Integer32	When this is set to 1, the device statement is released with a 0.
101	snmperrs (101)	-	Contains <code>snmpd</code> error information.
101.1	snmperrIndex (1)	Integer32	A fake index for <code>snmperrs</code> .
101.2	snmperrNames (2)	DisplayString	<code>Snmp</code>
101.100	snmperrErrorFlag (100)	UCDErrorFlag	An error flag indicating a problem with the agent. Each value represents the following: 0: noError, 1: error
101.101	snmperrErrorMessage (101)	DisplayString	A message explaining the problem.
<p>#1: These cannot be obtained.</p> <p>#2: The following is an example of how to calculate the capacity when <code>dskTotalLow</code> is 3431333888 and <code>dskTotalHigh</code> is 4872:</p> <ol style="list-style-type: none"> Convert the obtained MIB values to hexadecimal numbers. 3431333888 = 0xCC860000 4872 = 0x1308 Concatenate the hexadecimal <code>dskTotalHigh</code> in front of <code>dskTotalLow</code>. 0x1308, 0xCC860000 = 0x1308CC860000 Convert the concatenated number to a decimal number. 0x1308CC860000 = 2092851200000 (KB) 			

Table F-19 netSnmp (8072) group

ID	Object name	Type	Meaning
1	netSnmpObjects (1)	-	Objects for <code>netSnmp</code>

ID	Object name	Type	Meaning
1.2	nsMibRegistry (2)	-	Monitor for registered MIB modules
1.2.1	nsModuleTable (1)	-	Table displaying all OIDs registered by the MIB module
1.2.1.1	nsModuleEntry (1)	-	MIB module entry
1.2.1.1.1	nsmContextName (1)	-	Context name for the registered MIB module [#]
1.2.1.1.2	nsmRegistrationPoint (2)	-	OID for the registered MIB module [#]
1.2.1.1.3	nsmRegistrationPriority (3)	-	Priority for the registered MIB module [#]
1.2.1.1.4	nsModuleName (4)	DisplayString	Name of the registered MIB module
1.2.1.1.5	nsModuleModes (5)	BITS	Access attribute for the registered MIB module Each value represents the following: 0: getAndGetNext, 1: set, 2: getBulk
1.2.1.1.6	nsModuleTimeout (6)	Integer32	Timeout value for the registered MIB module
1.5	nsCache (5)	-	Objects related to saving SNMP agent data
1.5.1	nsCacheDefaultTimeout (1)	INTEGER	Initial save timeout value
1.5.2	nsCacheEnabled (2)	TruthValue	Whether save is enabled Each value represents the following: 1: true, 2: false
1.5.3	nsCacheTable (3)	-	Table for each MIB module and saved data
1.5.3.1	nsCacheEntry (1)	-	Conceptual entry in the save table
1.5.3.1.1	nsCachedOID (1)	-	OID for saved data [#]
1.5.3.1.2	nsCacheTimeout (2)	INTEGER	Entry-specific save timeout value
1.5.3.1.3	nsCacheStatus (3)	NetsnmpCacheStatus	Current status of entry-specific save Each value represents the following: 1: enabled, 2: disabled, 3: empty, 4: active, 5: empty
1.7	nsConfiguration (7)	-	Group for debugging and logging settings
1.7.1	nsConfigDebug (1)	-	Debugging settings (this is active if the debugging option is specified when <code>snmpd</code> is started)
1.7.1.1	nsDebugEnabled (1)	TruthValue	Setting used to output debugging information

ID	Object name	Type	Meaning
			Each value represents the following: 1: true, 2: false
1.7.1.2	nsDebugOutputAll (2)	TruthValue	Setting used to output all debugging information Each value represents the following: 1: true, 2: false
1.7.1.3	nsDebugDumpPdu (3)	TruthValue	Setting used to output packet dump information Each value represents the following: 1: true, 2: false
1.7.2	nsConfigLogging (2)	-	Logging settings (this is active if the logging option is specified when <code>snmpd</code> is started)
1.7.2.1	nsLoggingTable (1)	-	Logging output table
1.7.2.1.1	nsLoggingEntry (1)	-	Logging output entry
1.7.2.1.1.1	nsLogLevel (1)	INTEGER	(Minimum) priority level that should be applied for this logging entry# Each value represents the following: 0: emergency, 1: alert, 2: critical, 3: error, 4: warning, 5: notice, 6: info, 7: debug
1.7.2.1.1.2	nsLogToken (2)	DisplayString	Entry for where this entry is logged#
1.7.2.1.1.3	nsLogType (3)	INTEGER	Logging type for this entry Each value represents the following: 1: stdout, 2: stderr, 3: file, 4: syslog, 5: callback
1.7.2.1.1.4	nsLogMaxLevel (4)	INTEGER	Maximum priority level that should be applied for this logging entry Each value represents the following: 0: emergency, 1: alert, 2: critical, 3: error, 4: warning, 5: notice, 6: info, 7: debug
1.7.2.1.1.5	nsLogStatus (5)	RowStatus	Logging status Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
#: These cannot be obtained.			

Table F-20 snmpFrameworkMIB (10) group

ID	Object name	Type	Meaning
2	snmpFrameworkMIBObjects (2)	-	N/A
2.1	snmpEngine (1)	-	N/A
2.1.1	snmpEngineID (1)	SnmpEngineID	A unique identifier for SNMP engine operation.
2.1.2	snmpEngineBoots (2)	INTEGER	The number of times the SNMP engine was (re)initialized since <code>snmpEngineID</code> was last set.
2.1.3	snmpEngineTime (3)	INTEGER	The number of seconds that have elapsed since the value of <code>snmpEngineBoots</code> was last set.
2.1.4	snmpEngineMaxMessageSize (4)	INTEGER	The maximum octet length of SNMP messages that the SNMP engine can transmit and process (as dictated by the minimum value of the maximum size of messages that can be transmitted and processed by all transports).
Note: N/A = Not applicable.			

Table F-21 snmpMPDMIB (11) group

ID	Object name	Type	Meaning
2	snmpMPDMIBObjects (2)	-	N/A
2.1	snmpMPDStats (1)	-	N/A
2.1.1	snmpUnknownSecurityModels (1)	Counter32	The total number of packets received by the SNMP engine, not including those not supported by the SNMP engine.
2.1.2	snmpInvalidMsgs (2)	Counter32	The total number of packets received by the SNMP engine, not including invalid or inconsistent components in SNMP messages.
2.1.3	snmpUnknownPDUHandlers (3)	Counter32	The total number of packets received by the SNMP engine, not including those for which PDUs containing <code>pduType</code> packets could not be passed.
Note: N/A = Not applicable.			
These MIB information items are reset when SNMP agents are restarted. Because SNMP agents are restarted in an HDI system once a day, information for only one day is stored at most.			

Table F-22 snmpTargetMIB (12) group

ID	Object name	Type	Meaning
1	snmpTargetObjects (1)	-	N/A
1.2	snmpTargetAddrTable (2)	-	The transport table is used to create SNMP messages.
1.2.1	snmpTargetAddrEntry (1)	-	The transport address is used to create SNMP operations.
1.2.1.1	snmpTargetAddrName (1)	SnmpAdminString	A unique identifier that is locally optional but related to this <code>snmpTargetAddrEntry</code> .#
1.2.1.2	snmpTargetAddrTDomain (2)	TDomain	Indicates the address of the transport type included in the <code>snmpTargetAddrTAddress</code> object.
1.2.1.3	snmpTargetAddrTAddress (3)	TAddress	This address format, which contains the transport address, is dependent on the value of the <code>snmpTargetAddrTDomain</code> object.
1.2.1.4	snmpTargetAddrTimeout (4)	TimeInterval	This reflects the expected maximum round-trip time for contacting the transport address defined in this row.
1.2.1.5	snmpTargetAddrRetryCount (5)	Integer32	Specifies the default number of retries when a message, for which a response was created, cannot be received.
1.2.1.6	snmpTargetAddrTagList (6)	SnmpTagList	Contains the tag list used to choose the target address for a particular operation.
1.2.1.7	snmpTargetAddrParams (7)	SnmpAdminString	Identifies an entry from within the <code>snmpTargetParamsTable</code> .
1.2.1.8	snmpTargetAddrStorageType (8)	StorageType	The memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.2.1.9	snmpTargetAddrRowStatus (9)	RowStatus	The status. Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
1.3	snmpTargetParamsTable (3)	-	A table of SNMP target information used to create SNMP messages.
1.3.1	snmpTargetParamsEntry (1)	-	One piece of information for one SNMP set.
1.3.1.1	snmpTargetParamsName (1)	SnmpAdminString	A unique identifier that is locally optional but related to this <code>snmpTargetParamsEntry</code> .#

ID	Object name	Type	Meaning
1.3.1.2	snmpTargetParamsMPModel (2)	SnmpMessageProcessingModel	When this entry is used to create an SNMP message, a certain message processing module has been used.
1.3.1.3	snmpTargetParamsSecurityModel (3)	SnmpSecurityModel	The security models for the SNMP messages. Each value represents the following: 0: SNMP_SEC_MODEL_ANY, 1: SNMP_SEC_MODEL_SNMPv1, 2: SNMP_SEC_MODEL_SNMPv2c, 3: SNMP_SEC_MODEL_USM, 256: SNMP_SEC_MODEL_SNMPv2p
1.3.1.4	snmpTargetParamsSecurityName (4)	SnmpAdminString	The <code>securityName</code> specifying the principal in an SNMP message occurs using this entry.
1.3.1.5	snmpTargetParamsSecurityLevel (5)	SnmpSecurityLevel	The security level used when this entry is used to create an SNMP message. Each value represents the following: 1: noAuthNoPriv, 2: authNoPriv, 3: authPriv
1.3.1.6	snmpTargetParamsStorageType (6)	StorageType	The <code>nonVolatile</code> , <code>permanent</code> , or <code>readOnly</code> memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.3.1.7	snmpTargetParamsRowStatus (7)	RowStatus	When the value of this object is <code>active</code> (1), the following objects are not corrected: <ul style="list-style-type: none"> • <code>snmpTargetParamsMPModel</code> • <code>snmpTargetParamsSecurityModel</code> • <code>snmpTargetParamsSecurityName</code> • <code>snmpTargetParamsSecurityLevel</code> Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
Note: N/A = Not applicable. #: These cannot be obtained.			

Table F-23 snmpNotificationMIB (13) group

ID	Object name	Type	Meaning
1	snmpNotifyObjects (1)	-	N/A

ID	Object name	Type	Meaning
1.1	snmpNotifyTable (1)	-	Contains the object selecting the host and notification type.
1.1.1	snmpNotifyEntry (1)	-	Used to configure the notification entry.
1.1.1.1	snmpNotifyName (1)	SnmpAdminString	Indicates the notification name.#
1.1.1.2	snmpNotifyTag (2)	SnmpTagValue	Used to select entries in the snmpTargetAddrTable.
1.1.1.3	snmpNotifyType (3)	INTEGER	This is 1 in case of a trap, or 2 in case of a notification. Each value represents the following: 1: trap, 2: inform
1.1.1.4	snmpNotifyStorageType (4)	StorageType	nonVolatile, permanent, or readOnly. Each value represents the following: 1: other, 2: volatile, 3: nonVolatile, 4: permanent, 5: readOnly
1.1.1.5	snmpNotifyRowStatus (5)	RowStatus	The status of the row of this overview. Each value represents the following: 1: active, 2: notInService, 3: notReady, 4: createAndGo, 5: createAndWait, 6: destroy
Note: N/A = Not applicable. #: These cannot be obtained.			

Table F-24 snmpUsmMIB (15) group

ID	Object name	Type	Meaning
1	usmMIBObjects (1)	-	N/A
1.1	usmStats (1)	-	N/A
1.1.1	usmStatsUnsupportedSecurityLevels (1)	Counter32	The total number of packets received by the SNMP engine, not including cases in which a securityLevel that is not used or not in the SNMP engine was requested.
1.1.2	usmStatsNotInTimeWindows (2)	Counter32	The total number of packets received by the SNMP engine, not including those appearing outside of the SNMP engine.
1.1.3	usmStatsUnknownUserNames (3)	Counter32	The total number of packets received by the SNMP engine, not including user views of which the SNMP engine was not notified.
1.1.4	usmStatsUnknownEngineIDs (4)	Counter32	The total number of packets received by the SNMP engine, not

ID	Object name	Type	Meaning
			including <code>snmpEngineIDs</code> of which the SNMP engine was not notified.
1.1.5	<code>usmStatsWrongDigests</code> (5)	Counter32	The total number of packets received by the SNMP engine, not including those that did not have an expected digest value.
1.1.6	<code>usmStatsDecryptionErrors</code> (6)	Counter32	The total number of packets received by the SNMP engine, not including those that could not be decrypted.
1.2	<code>usmUser</code> (2)	-	N/A
1.2.1	<code>usmUserSpinLock</code> (1)	TestAndIncr	Locks are used so that the various cooperating command generator applications can be reconciled.
<p>Note: N/A = Not applicable.</p> <p>These MIB information items are reset when SNMP agents are restarted. Because SNMP agents are restarted in an HDI system once a day, information for only 1 day is stored at most.</p>			

Table F-25 `snmpVacmMIB` (16) group

ID	Object name	Type	Meaning
1	<code>vacmMIBObjects</code> (1)	-	N/A
1.2	<code>vacmSecurityToGroupTable</code> (2)	-	A table used so that the access management policy for the combination of <code>securityModel</code> and <code>securityName</code> can be defined for the primary group. This is mapped to <code>groupName</code> .
1.2.1	<code>vacmSecurityToGroupEntry</code> (1)	-	Used to allocate principals to the group.
1.2.1.1	<code>vacmSecurityModel</code> (1)	-	The security model.#
1.2.1.2	<code>vacmSecurityName</code> (2)	-	The security name.#
1.2.1.3	<code>vacmGroupName</code> (3)	SnmpAdminString	Group name.
1.2.1.4	<code>vacmSecurityToGroupStorageType</code> (4)	StorageType	The memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.2.1.5	<code>vacmSecurityToGroupStatus</code> (5)	RowStatus	The status. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.4	<code>vacmAccessTable</code> (4)	-	The access permissions table.

ID	Object name	Type	Meaning
1.4.1	vacmAccessEntry (1)	-	The access permissions configured in the Local Configuration Datastore (LCD) permitting access to SNMP.
1.4.1.1	vacmAccessContextPrefix (1)	-	The value of this object must match <code>contextName</code> , so that access permissions can be obtained.#
1.4.1.2	vacmAccessSecurityModel (2)	-	This <code>securityModel</code> must be used to obtain access permissions.#
1.4.1.3	vacmAccessSecurityLevel (3)	-	The minimum security level.#
1.4.1.4	vacmAccessContextMatch (4)	INTEGER	The method by which the context for <code>exact</code> or <code>prefix</code> requests matches <code>vacmAccessContextPrefix</code> . Each value represents the following: 1: exact, 2: prefix
1.4.1.5	vacmAccessReadViewName (5)	SnmpAdminString	Used to define the view subtree for <code>GetRequests</code> .
1.4.1.6	vacmAccessWriteViewName (6)	SnmpAdminString	Used to define the view subtree for <code>SetRequests</code> .
1.4.1.7	vacmAccessNotifyViewName (7)	SnmpAdminString	Used to define the view subtree so that objects within trap messages and <code>InformRequests</code> can be loaded as <code>VarBinds</code> .
1.4.1.8	vacmAccessStorageType (8)	StorageType	The memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.4.1.9	vacmAccessStatus (9)	RowStatus	The status. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.5	vacmMIBViews (5)	-	N/A
1.5.1	vacmViewSpinLock (1)	TestAndIncr	Locks enable set operation usage to be adjusted when SNMP command generators are used to create or modify a view.
1.5.2	vacmViewTreeFamilyTable (2)	-	Locally stored information about a family of a subtree in MIB.
1.5.2.1	vacmViewTreeFamilyEntry (1)	-	Information about a particular family of a subtree.
1.5.2.1.1	vacmViewTreeFamilyViewName (1)	SnmpAdminString	The human-readable name of family of the view subtree.#

ID	Object name	Type	Meaning
1.5.2.1.2	vacmViewTreeFamilySubtree (2)	-	The MIB subtree that defines the family of the view subtree for vacmViewTreeFamilyMask.#
1.5.2.1.3	vacmViewTreeFamilyMask (3)	OCTET STRING	The mask that defines the family of the view subtree for vacmViewTreeFamilySubtree.
1.5.2.1.4	vacmViewTreeFamilyType (4)	INTEGER	Indicates whether or not the subtree under the OID defined in vacmViewTreeFamilySubtree can be accessed. Each value represents the following: 1: include, 2: exclude
1.5.2.1.5	vacmViewTreeFamilyStorageType (5)	StorageType	The memory type. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
1.5.2.1.6	vacmViewTreeFamilyStatus (6)	RowStatus	The status. Each value represents the following: 1: other, 2: volatile, 3: nonvolatile, 4: permanent, 5: readOnly
Note: N/A = Not applicable. #: These cannot be obtained.			

Table F-26 stdExMibQuotaTable (2) group

ID	Object name	Type	Meaning
1	quotaEntry (1)	-	Quota management information for each file system
1.1	quotaFSIndex (1)	INTEGER	The index number that corresponds to the file system
1.2	quotaFSMntPoint (2)	DisplayString	The mount point for the file system
1.3	quotaFSBlockMaxGrace (3)	INTEGER	The grace period (number of days) when the number of blocks exceeds the soft limit
1.4	quotaFSFileMaxGrace (4)	INTEGER	The grace period (number of days) when the number of inodes exceeds the soft limit
1.5	quotaFSStatus (5)	INTEGER	Quota status (off/on) Each value represents the following: 0: off, 1: on, 2: group-on, 3: user-on
1.6	quotaFSUserTable (6)	-	Information about quota management for users

ID	Object name	Type	Meaning
1.6.1	quotaUserEntry (1)	-	Information about quota management for each user
1.6.1.1	quotaUserIndex (1)	Integer32	Index number for a user
1.6.1.2	quotaUserUID (2)	Integer32	UID
1.6.1.3	quotaUserBlockCount (3)	INTEGER	The number (KB) of blocks being used
1.6.1.4	quotaUserFileCount (4)	INTEGER	The number of inodes being used
1.6.1.5	quotaUserBlockSoftLimit (5)	INTEGER	The soft limit for the number of blocks
1.6.1.6	quotaUserFileSoftLimit (6)	INTEGER	The soft limit for the number of inodes
1.6.1.7	quotaUserBlockHardLimit (7)	INTEGER	The hard limit for the number of blocks
1.6.1.8	quotaUserFileHardLimit (8)	INTEGER	The hard limit for the number of inodes
1.6.1.9	quotaUserBlockGracePeriod (9)	Counter32	Time (seconds) remaining for the grace period from when the number of blocks exceeded the soft limit
1.6.1.10	quotaUserFileGracePeriod (10)	Counter32	Time (seconds) remaining for the grace period from when the number of inodes exceeded the soft limit
1.6.1.11	quotaUserBlockGracePeriodOver (11)	DisplayString	Outputs "over" when the grace period for the number of blocks exceeding the soft limit is expired.
1.6.1.12	quotaUserFileGracePeriodOver (12)	DisplayString	Outputs "over" when the grace period for the number of inodes exceeding the soft limit is expired.
1.6.1.13	quotaUser64UsedCount (13)	Counter64	The number of blocks used (64-bit compatible) (KB)
1.6.1.14	quotaUser64UsedMBCount (14)	Counter64	The number of blocks used (64-bit compatible) (MB)
1.6.1.15	quotaUser64UsedGBCount (15)	Counter64	The number of blocks used (64-bit compatible) (GB)
1.6.1.16	quotaUser64FileCount (16)	Counter64	The number of inodes used (64-bit compatible)
1.6.1.17	quotaUser64UsedSoftLimit (17)	Counter64	The soft limit for the number of blocks (64-bit compatible) (KB)
1.6.1.18	quotaUser64UsedMBSoftLimit (18)	Counter64	The soft limit for the number of blocks (64-bit compatible) (MB)
1.6.1.19	quotaUser64UsedGBSoftLimit (19)	Counter64	The soft limit for the number of blocks (64-bit compatible) (GB)
1.6.1.20	quotaUser64FileSoftLimit (20)	Counter64	The soft limit for the number of inodes (64-bit compatible)

ID	Object name	Type	Meaning
1.6.1.2 1	quotaUser64UsedHardLimit (21)	Counter64	The hard limit for the number of blocks (64-bit compatible) (KB)
1.6.1.2 2	quotaUser64UsedMBHardLimit (22)	Counter64	The hard limit for the number of blocks (64-bit compatible) (MB)
1.6.1.2 3	quotaUser64UsedGBHardLimit (23)	Counter64	The hard limit for the number of blocks (64-bit compatible) (GB)
1.6.1.2 4	quotaUser64FileHardLimit (24)	Counter64	The hard limit for the number of inodes (64-bit compatible)
1.7	quotaFSGroupTable (7)	-	Information about quota management for groups
1.7.1	quotaGroupEntry (1)	-	Information about quota management for each group
1.7.1.1	quotaGroupIndex (1)	Integer32	Index number for a group
1.7.1.2	quotaGroupGID (2)	Integer32	GID
1.7.1.3	quotaGroupBlockCount (3)	INTEGER	The number (KB) of blocks being used
1.7.1.4	quotaGroupFileCount (4)	INTEGER	The number of inodes being used
1.7.1.5	quotaGroupBlockSoftLimit (5)	INTEGER	The soft limit for the number of blocks
1.7.1.6	quotaGroupFileSoftLimit (6)	INTEGER	The soft limit for the number of inodes
1.7.1.7	quotaGroupBlockHardLimit (7)	INTEGER	The hard limit for the number of blocks
1.7.1.8	quotaGroupFileHardLimit (8)	INTEGER	The hard limit for the number of inodes
1.7.1.9	quotaGroupBlockGracePeriod (9)	Counter32	Time (seconds) remaining for the grace period from when the number of blocks exceeded the soft limit
1.7.1.10	quotaGroupFileGracePeriod (10)	Counter32	Time (seconds) remaining for the grace period from when the number of inodes exceeded the soft limit
1.7.1.11	quotaGroupBlockGracePeriodOver (11)	DisplayString	Displays "over" when the grace period is passed for the number of blocks exceeding the soft limit
1.7.1.12	quotaGroupFileGracePeriodOver (12)	DisplayString	Displays "over" when the grace period is passed for the number of inodes exceeding the soft limit
1.7.1.13	quotaGroup64UsedCount (13)	Counter64	The number of blocks used (64-bit compatible) (KB)
1.7.1.14	quotaGroup64UsedMBCount (14)	Counter64	The number of blocks used (64-bit compatible) (MB)
1.7.1.15	quotaGroup64UsedGBCount (15)	Counter64	The number of blocks used (64-bit compatible) (GB)

ID	Object name	Type	Meaning
1.7.1.1.6	quotaGroup64FileCount (16)	Counter64	The number of inodes being used (for 64bit)
1.7.1.1.7	quotaGroup64UsedSoftLimit (17)	Counter64	The soft limit for the used capacity (for 64bit) (KB)
1.7.1.1.8	quotaGroup64UsedMBSoftLimit (18)	Counter64	The soft limit for the used capacity (for 64bit) (MB)
1.7.1.1.9	quotaGroup64UsedGBSoftLimit (19)	Counter64	The soft limit for the used capacity (for 64bit) (GB)
1.7.1.2.0	quotaGroup64FileSoftLimit (20)	Counter64	The soft limit for the number of inodes (for 64bit)
1.7.1.2.1	quotaGroup64UsedHardLimit (21)	Counter64	The hard limit for the used capacity (for 64bit) (KB)
1.7.1.2.2	quotaGroup64UsedMBHardLimit (22)	Counter64	The hard limit for the used capacity (for 64bit) (MB)
1.7.1.2.3	quotaGroup64UsedGBHardLimit (23)	Counter64	The hard limit for the used capacity (for 64bit) (GB)
1.7.1.2.4	quotaGroup64FileHardLimit (24)	Counter64	The hard limit for the number of inodes (for 64bit)
2	quotaSubtreeEntry (2)	-	The subtree quota management information set for the directory
2.1	quotaSubtreeDirIndex (1)	INTEGER	The index number of the directory table
2.2	quotaSubtreeDirPath (2)	OCTET STRING	The directory path
2.3	quotaSubtreeDirUsed (3)	Counter64	The used capacity of the subtree quota (KB)
2.4	quotaSubtreeDirFileCount (4)	Counter64	The number of inodes being used
2.5	quotaSubtreeDirUsedSoftLimit (5)	Counter64	The soft limit for the used capacity (KB)
2.6	quotaSubtreeDirUsedMBSoftLimit (6)	Counter64	The soft limit for the used capacity (MB)
2.7	quotaSubtreeDirUsedGBSoftLimit (7)	Counter64	The soft limit for the used capacity (GB)
2.8	quotaSubtreeDirFileSoftLimit (8)	Counter64	The soft limit for the number of inodes
2.9	quotaSubtreeDirUsedHardLimit (9)	Counter64	The hard limit for the used capacity (KB)
2.10	quotaSubtreeDirUsedMBHardLimit (10)	Counter64	The hard limit for the used capacity (MB)
2.11	quotaSubtreeDirUsedGBHardLimit (11)	Counter64	The hard limit for the used capacity (GB)

ID	Object name	Type	Meaning
2.12	quotaSubtreeDirFileHardLimit (12)	Counter64	The hard limit for the number of inodes
2.13	quotaSubtreeDirUsedSoftLimitPercent (13)	INTEGER	The used capacity as a percentage of the soft limit for the used capacity
2.14	quotaSubtreeDirFileSoftLimitPercent (14)	INTEGER	The number of inodes as a percentage of the soft limit for the number of inodes
2.15	quotaSubtreeDirUsedHardLimitPercent (15)	INTEGER	The used capacity as a percentage of the hard limit for the used capacity
2.16	quotaSubtreeDirFileHardLimitPercent (16)	INTEGER	The number of inodes as a percentage of the hard limit for the number of inodes
2.17	quotaSubtreeDirUsedGracePeriod (17)	Counter32	The set grace period during which the soft limit for the used capacity can be exceeded (seconds)
2.18	quotaSubtreeDirFileGracePeriod (18)	Counter32	The set grace period during which the soft limit for the number of inodes can be exceeded (seconds)
2.19	quotaSubtreeUserTable (19)#	-	The user subtree quota management information
2.19.1	quotaSubtreeUserEntry (1)	-	The subtree quota management information for each user
2.19.1.1	quotaSubtreeUserIndex (1)	Integer32	The index number of the user ID
2.19.1.2	quotaSubtreeUserUID (2)	INTEGER	The user ID
2.19.1.3	quotaSubtreeUserUsed (3)	Counter64	The used capacity of the subtree quota (KB)
2.19.1.4	quotaSubtreeUserFileCount (4)	Counter64	The number of inodes being used
2.19.1.5	quotaSubtreeUserUsedSoftLimit (5)	Counter64	The soft limit for the used capacity (KB)
2.19.1.6	quotaSubtreeUserUsedMBSoftLimit (6)	Counter64	The soft limit for the used capacity (MB)
2.19.1.7	quotaSubtreeUserUsedGBSoftLimit (7)	Counter64	The soft limit for the used capacity (GB)
2.19.1.8	quotaSubtreeUserFileSoftLimit (8)	Counter64	The soft limit for the number of inodes
2.19.1.9	quotaSubtreeUserUsedHardLimit (9)	Counter64	The hard limit for the used capacity (KB)
2.19.1.10	quotaSubtreeUserUsedMBHardLimit (10)	Counter64	The hard limit for the used capacity (MB)
2.19.1.11	quotaSubtreeUserUsedGBHardLimit (11)	Counter64	The hard limit for the used capacity (GB)

ID	Object name	Type	Meaning
2.19.1.12	quotaSubtreeUserFileHardLimit (12)	Counter64	The hard limit for the number of inodes
2.19.1.13	quotaSubtreeUserUsedSoftLimitPercent (13)	INTEGER	The used capacity as a percentage of the soft limit for the used capacity
2.19.1.14	quotaSubtreeUserFileSoftLimitPercent (14)	INTEGER	The number of inodes as a percentage of the soft limit for the number of inodes
2.19.1.15	quotaSubtreeUserUsedHardLimitPercent (15)	INTEGER	The used capacity as a percentage of the hard limit for the used capacity
2.19.1.16	quotaSubtreeUserFileHardLimitPercent (16)	INTEGER	The number of inodes as a percentage of the hard limit for the number of inodes
2.19.1.17	quotaSubtreeUserUsedGracePeriod (17)	Counter32	The set grace period during which the soft limit for the used capacity can be exceeded (seconds)
2.19.1.18	quotaSubtreeUserFileGracePeriod (18)	Counter32	The set grace period during which the soft limit for the number of inodes can be exceeded (seconds)
2.19.1.19	quotaSubtreeUserUsedGracePeriodOver (19)	DisplayString	Displays "over" when the grace period is passed for the number of blocks exceeding the soft limit
2.19.1.20	quotaSubtreeUserFileGracePeriodOver (20)	DisplayString	Displays "over" when the grace period is passed for the number of inodes exceeding the soft limit
2.19.1.21	quotaSubtreeUserUsedMB (21)	Counter64	The used capacity of the subtree quota (MB)
2.19.1.22	quotaSubtreeUserUsedGB (22)	Counter64	The used capacity of the subtree quota (GB)
2.20	quotaSubtreeGroupTable (20)#	-	The group subtree quota management information
2.20.1	quotaSubtreeGroupEntry (1)	-	The subtree quota management information for each group
2.20.1.1	quotaSubtreeGroupIndex (1)	Integer32	The index number for the group
2.20.1.2	quotaSubtreeGroupGID (2)	INTEGER	The group ID
2.20.1.3	quotaSubtreeGroupUsed (3)	Counter64	The used capacity of the subtree quota (KB)
2.20.1.4	quotaSubtreeGroupFileCount (4)	Counter64	The number of inodes being used
2.20.1.5	quotaSubtreeGroupUsedSoftLimit (5)	Counter64	The soft limit for the used capacity (KB)
2.20.1.6	quotaSubtreeGroupUsedMBSLimit (6)	Counter64	The soft limit for the used capacity (MB)

ID	Object name	Type	Meaning
2.20.1.7	quotaSubtreeGroupUsedGBSoftLimit (7)	Counter64	The soft limit for the used capacity (GB)
2.20.1.8	quotaSubtreeGroupFileSoftLimit (8)	Counter64	The soft limit for the number of inodes
2.20.1.9	quotaSubtreeGroupUsedHardLimit (9)	Counter64	The hard limit for the used capacity (KB)
2.20.1.10	quotaSubtreeGroupUsedMBHardLimit (10)	Counter64	The hard limit for the used capacity (MB)
2.20.1.11	quotaSubtreeGroupUsedGBHardLimit (11)	Counter64	The hard limit for the used capacity (GB)
2.20.1.12	quotaSubtreeGroupFileHardLimit (12)	Counter64	The hard limit for the number of inodes
2.20.1.13	quotaSubtreeGroupUsedSoftLimitPercent (13)	INTEGER	The used capacity as a percentage of the soft limit for the used capacity
2.20.1.14	quotaSubtreeGroupFileSoftLimitPercent (14)	INTEGER	The number of inodes as a percentage of the soft limit for the number of inodes
2.20.1.15	quotaSubtreeGroupUsedHardLimitPercent (15)	INTEGER	The used capacity as a percentage of the hard limit for the used capacity
2.20.1.16	quotaSubtreeGroupFileHardLimitPercent (16)	INTEGER	The number of inodes as a percentage of the hard limit for the number of inodes
2.20.1.17	quotaSubtreeGroupUsedGracePeriod (17)	Counter32	The set grace period during which the soft limit for the used capacity can be exceeded (seconds)
2.20.1.18	quotaSubtreeGroupFileGracePeriod (18)	Counter32	The set grace period during which the soft limit for the number of inodes can be exceeded (seconds)
2.20.1.19	quotaSubtreeGroupUsedGracePeriodOver (19)	DisplayString	Displays "over" when the grace period is passed for the number of blocks exceeding the soft limit
2.20.1.20	quotaSubtreeGroupFileGracePeriodOver (20)	DisplayString	Displays "over" when the grace period is passed for the number of inodes exceeding the soft limit
2.20.1.21	quotaSubtreeGroupUsedMB (21)	Counter64	The used capacity of the subtree quota (MB)
2.20.1.22	quotaSubtreeGroupUsedGB (22)	Counter64	The used capacity of the subtree quota (GB)
2.21	quotaSubtreeDirUsedGracePeriodOver (21)	DisplayString	Displays "over" when the grace period is passed for the number of blocks exceeding the soft limit
2.22	quotaSubtreeDirFileGracePeriodOver (22)	DisplayString	Displays "over" when the grace period is passed for the number of inodes exceeding the soft limit

ID	Object name	Type	Meaning
2.23	quotaSubtreeDirUsedMB (23)	Counter64	The used capacity of the subtree quota (MB)
2.24	quotaSubtreeDirUsedGB (24)	Counter64	The used capacity of the subtree quota (GB)
#: If multiple subtree quotas are set for the tree of directories that have parent-child relationships (from top to bottom), MIB objects are acquired only for the lowest subtree quota in that directory tree.			

Table F-27 stdExMibNfs (4) group

ID	Object name	Type	Meaning
1	stdExMibNfsRpcStats (1)	-	Number of RPC requests since system activation
1.1	nfsCALLS (1)	Counter32	The total number of RPC requests
1.2	nfsBADCALLS (2)	Counter32	The number of requests deleted in the RPC layer
1.3	nfsXDRCALL (3)	Counter32	The number of requests that have headers that XDR cannot decipher
2	stdExMibNfsV2ProcCall (2)	-	Number of received NFSv2 procedure calls
2.1	nfsV2ProcNULL (1)	Counter32	The number of received NULL procedure calls
2.2	nfsV2ProcGETATTR (2)	Counter32	The number of received GETATTR procedure calls
2.3	nfsV2ProcSETATTR (3)	Counter32	The number of received SETATTR procedure calls
2.4	nfsV2ProcROOT (4)	Counter32	The number of received ROOT procedure calls
2.5	nfsV2ProcLOOKUP (5)	Counter32	The number of received LOOKUP procedure calls
2.6	nfsV2ProcREADLINK (6)	Counter32	The number of received READLINK procedure calls
2.7	nfsV2ProcREAD (7)	Counter32	The number of received READ procedure calls
2.8	nfsV2ProcWRITECACHE (8)	Counter32	The number of received WRITECACHE procedure calls
2.9	nfsV2ProcWRITE (9)	Counter32	The number of received WRITE procedure calls
2.10	nfsV2ProcCREATE (10)	Counter32	The number of received CREATE procedure calls
2.11	nfsV2ProcREMOVE (11)	Counter32	The number of received REMOVE procedure calls

ID	Object name	Type	Meaning
2.12	nfsV2ProcRENAME (12)	Counter32	The number of received RENAME procedure calls
2.13	nfsV2ProcLINK (13)	Counter32	The number of received LINK procedure calls
2.14	nfsV2ProcSYMLINK (14)	Counter32	The number of received SYMLINK procedure calls
2.15	nfsV2ProcMKDIR (15)	Counter32	The number of received MKDIR procedure calls
2.16	nfsV2ProcRMDIR (16)	Counter32	The number of received RMDIR procedure calls
2.17	nfsV2ProcREaddir (17)	Counter32	The number of received REaddir procedure calls
2.18	nfsV2ProcFSSTAT (18)	Counter32	The number of received FSSTAT procedure calls
3	stdExMibNfsV2TotalProcCall (3)	-	Statistics of individual NFSv2 calls (in %)
3.1	nfsV2TotalProcNULL (1)	INTEGER	Statistics (%) for NULL procedure calls
3.2	nfsV2TotalProcGETATTR (2)	INTEGER	Statistics (%) for GETATTR procedure calls
3.3	nfsV2TotalProcSETATTR (3)	INTEGER	Statistics (%) for SETATTR procedure calls
3.4	nfsV2TotalProcROOT (4)	INTEGER	Statistics (%) for ROOT procedure calls
3.5	nfsV2TotalProcLOOKUP (5)	INTEGER	Statistics (%) for LOOKUP procedure calls
3.6	nfsV2TotalProcREADLINK (6)	INTEGER	Statistics (%) for READLINK procedure calls
3.7	nfsV2TotalProcREAD (7)	INTEGER	Statistics (%) for READ procedure calls
3.8	nfsV2TotalProcWRITECACHE (8)	INTEGER	Statistics (%) for WRITECACHE procedure calls
3.9	nfsV2TotalProcWRITE (9)	INTEGER	Statistics (%) for WRITE procedure calls
3.10	nfsV2TotalProcCREATE (10)	INTEGER	Statistics (%) for CREATE procedure calls
3.11	nfsV2TotalProcREMOVE (11)	INTEGER	Statistics (%) for REMOVE procedure calls
3.12	nfsV2TotalProcRENAME (12)	INTEGER	Statistics (%) for RENAME procedure calls
3.13	nfsV2TotalProcLINK (13)	INTEGER	Statistics (%) for LINK procedure calls

ID	Object name	Type	Meaning
3.14	nfsV2TotalProcSYMLINK (14)	INTEGER	Statistics (%) for SYMLINK procedure calls
3.15	nfsV2TotalProcMKDIR (15)	INTEGER	Statistics (%) for MKDIR procedure calls
3.16	nfsV2TotalProcRMDIR (16)	INTEGER	Statistics (%) for RMDIR procedure calls
3.17	nfsV2TotalProcREADDIR (17)	INTEGER	Statistics (%) for READDIR procedure calls
3.18	nfsV2TotalProcFSSTAT (18)	INTEGER	Statistics (%) for FSSTAT procedure calls
4	stdExMibNfsV3ProcCall (4)	-	Number of received NFSv3 procedure calls
4.1	nfsV3ProcNULL (1)	Counter32	The number of received NULL procedure calls
4.2	nfsV3ProcGETATTR (2)	Counter32	The number of received GETATTR procedure calls
4.3	nfsV3ProcSETATTR (3)	Counter32	The number of received SETATTR procedure calls
4.4	nfsV3ProcLOOKUP (4)	Counter32	The number of received LOOKUP procedure calls
4.5	nfsV3ProcACCESS (5)	Counter32	The number of received ACCESS procedure calls
4.6	nfsV3ProcREADLINK (6)	Counter32	The number of received READLINK procedure calls
4.7	nfsV3ProcREAD (7)	Counter32	The number of received READ procedure calls
4.8	nfsV3ProcWRITE (8)	Counter32	The number of received WRITE procedure calls
4.9	nfsV3ProcCREATE (9)	Counter32	The number of received CREATE procedure calls
4.10	nfsV3ProcMKDIR (10)	Counter32	The number of received WRITECACHE procedure calls
4.11	nfsV3ProcSYMLINK (11)	Counter32	The number of received SYMLINK procedure calls
4.12	nfsV3ProcMKNOD (12)	Counter32	The number of received MKNOD procedure calls
4.13	nfsV3ProcREMOVE (13)	Counter32	The number of received REMOVE procedure calls
4.14	nfsV3ProcRMDIR (14)	Counter32	The number of received RMDIR procedure calls
4.15	nfsV3ProcRENAME (15)	Counter32	The number of received RENAME procedure calls

ID	Object name	Type	Meaning
4.16	nfsV3ProcLINK (16)	Counter32	The number of received LINK procedure calls
4.17	nfsV3ProcREaddir (17)	Counter32	The number of received REaddir procedure calls
4.18	nfsV3ProcREaddirPLUS (18)	Counter32	The number of received REaddirPLUS procedure calls
4.19	nfsV3ProcFSSTAT (19)	Counter32	The number of received FSSTAT procedure calls
4.20	nfsV3ProcFSINFO (20)	Counter32	The number of received FSINFO procedure calls
4.21	nfsV3ProcPATHCONF (21)	Counter32	The number of received PATHCONF procedure calls
4.22	nfsV3ProcCOMMIT (22)	Counter32	The number of received COMMIT procedure calls
5	stdExMibNfsV3TotalProcCall (5)	-	Statistics of individual NFSv3 calls (in %)
5.1	nfsV3TotalProcNULL (1)	INTEGER	Statistics (%) for NULL procedure calls
5.2	nfsV3TotalProcGETATTR (2)	INTEGER	Statistics (%) for GETATTR procedure calls
5.3	nfsV3TotalProcSETATTR (3)	INTEGER	Statistics (%) for SETATTR procedure calls
5.4	nfsV3TotalProcLOOKUP (4)	INTEGER	Statistics (%) for LOOKUP procedure calls
5.5	nfsV3TotalProcACCESS (5)	INTEGER	Statistics (%) for ACCESS procedure calls
5.6	nfsV3TotalProcREADLINK (6)	INTEGER	Statistics (%) for READLINK procedure calls
5.7	nfsV3TotalProcREAD (7)	INTEGER	Statistics (%) for READ procedure calls
5.8	nfsV3TotalProcWRITE (8)	INTEGER	Statistics (%) for WRITE procedure calls
5.9	nfsV3TotalProcCREATE (9)	INTEGER	Statistics (%) for CREATE procedure calls
5.10	nfsV3TotalProcMKDIR (10)	INTEGER	Statistics (%) for MKDIR procedure calls
5.11	nfsV3TotalProcSYMLINK (11)	INTEGER	Statistics (%) for SYMLINK procedure calls
5.12	nfsV3TotalProcMKNOD (12)	INTEGER	Statistics (%) for MKNOD procedure calls
5.13	nfsV3TotalProcREMOVE (13)	INTEGER	Statistics (%) for REMOVE procedure calls

ID	Object name	Type	Meaning
5.14	nfsV3TotalProcRMDIR (14)	INTEGER	Statistics (%) for RMDIR procedure calls
5.15	nfsV3TotalProcRENAME (15)	INTEGER	Statistics (%) for RENAME procedure calls
5.16	nfsV3TotalProcLINK (16)	INTEGER	Statistics (%) for LINK procedure calls
5.17	nfsV3TotalProcREADDIR (17)	INTEGER	Statistics (%) for READDIR procedure calls
5.18	nfsV3TotalProcREADDIRPLUS (18)	INTEGER	Statistics (%) for READDIRPLUS procedure calls
5.19	nfsV3TotalProcFSSTAT (19)	INTEGER	Statistics (%) for FSSTAT procedure calls
5.20	nfsV3TotalProcFSINFO (20)	INTEGER	Statistics (%) for FSINFO procedure calls
5.21	nfsV3TotalProcPATHCONF (21)	INTEGER	Statistics (%) for PATHCONF procedure calls
5.22	nfsV3TotalProcCOMMIT (22)	INTEGER	Statistics (%) for COMMIT procedure calls
6	stdExMibNfsV4Call (6)	-	Number of received NFSv4 procedure calls or operations
6.1	nfsV4ProcNULL (1)	Counter32	Number of received NULL procedure calls
6.2	nfsV4ProcCOMPOUND (2)	Counter32	Number of received COMPOUND procedure calls
6.3	nfsV4OperACCESS (3)	Counter32	Number of received ACCESS operations
6.4	nfsV4OperCLOSE (4)	Counter32	Number of received CLOSE operations
6.5	nfsV4OperCOMMIT (5)	Counter32	Number of received COMMIT operations
6.6	nfsV4OperCREATE (6)	Counter32	Number of received CREATE operations
6.7	nfsV4OperDELEGPURGE (7)	Counter32	Number of received DELEGPURGE operations
6.8	nfsV4OperDELEGRETURN (8)	Counter32	Number of received DELEGRETURN operations
6.9	nfsV4OperGETATTR (9)	Counter32	Number of received GETATTR operations
6.10	nfsV4OperGETFH (10)	Counter32	Number of received GETFH operations
6.11	nfsV4OperLINK (11)	Counter32	Number of received LINK operations

ID	Object name	Type	Meaning
6.12	nfsV4OperLOCK (12)	Counter32	Number of received LOCK operations
6.13	nfsV4OperLOCKT (13)	Counter32	Number of received LOCKT operations
6.14	nfsV4OperLOCKU (14)	Counter32	Number of received LOCKU operations
6.15	nfsV4OperLOOKUP (15)	Counter32	Number of received LOOKUP operations
6.16	nfsV4OperLOOKUPROOT (16)	Counter32	Number of received LOOKUPROOT operations
6.17	nfsV4OperNVERIFY (17)	Counter32	Number of received NVERIFY operations
6.18	nfsV4OperOPEN (18)	Counter32	Number of received OPEN operations
6.19	nfsV4OperOPENATTR (19)	Counter32	Number of received OPENATTR operations
6.20	nfsV4OperOPENCONF (20)	Counter32	Number of received OPENCONF operations
6.21	nfsV4OperOPENDGRD (21)	Counter32	Number of received OPENDGRD operations
6.22	nfsV4OperPUTFH (22)	Counter32	Number of received PUTFH operations
6.23	nfsV4OperPUTPUBFH (23)	Counter32	Number of received PUTPUBFH operations
6.24	nfsV4OperPUTROOTFH (24)	Counter32	Number of received PUTROOTFH operations
6.25	nfsV4OperREAD (25)	Counter32	Number of received READ operations
6.26	nfsV4OperREADDIR (26)	Counter32	Number of received READDIR operations
6.27	nfsV4OperREADLINK (27)	Counter32	Number of received READLINK operations
6.28	nfsV4OperREMOVE (28)	Counter32	Number of received REMOVE operations
6.29	nfsV4OperRENAME (29)	Counter32	Number of received RENAME operations
6.30	nfsV4OperRENEW (30)	Counter32	Number of received RENEW operations
6.31	nfsV4OperRESTOREFH (31)	Counter32	Number of received RESTOREFH operations
6.32	nfsV4OperSAVEFH (32)	Counter32	Number of received SAVEFH operations

ID	Object name	Type	Meaning
6.33	nfsV4OperSECINFO (33)	Counter32	Number of received SECINFO operations
6.34	nfsV4OperSETATTR (34)	Counter32	Number of received SETATTR operations
6.35	nfsV4OperSETCLTID (35)	Counter32	Number of received SETCLTID operations
6.36	nfsV4OperSETCLTIDCONF (36)	Counter32	Number of received SETCLTIDCONF operations
6.37	nfsV4OperVERIFY (37)	Counter32	Number of received VERIFY operations
6.38	nfsV4OperWRITE (38)	Counter32	Number of received WRITE operations
6.39	nfsV4OperRELOCKOWNER (39)	Counter32	Number of received RELOCKOWNER operations
7	stdExMibNfsV4TotalCall (7)	-	Statistics (%) based on the number of received NFSv4 total procedure calls or total operations as the parameter
7.1	nfsV4TotalProcNULL (1)	INTEGER	Statistics (%) for NULL procedure calls
7.2	nfsV4TotalProcCOMPOUND (2)	INTEGER	Statistics (%) for COMPOUND procedure calls
7.3	nfsV4TotalOperACCESS (3)	INTEGER	Statistics (%) for ACCESS operations
7.4	nfsV4TotalOperCLOSE (4)	INTEGER	Statistics (%) for CLOSE operations
7.5	nfsV4TotalOperCOMMIT (5)	INTEGER	Statistics (%) for COMMIT operations
7.6	nfsV4TotalOperCREATE (6)	INTEGER	Statistics (%) for CREATE operations
7.7	nfsV4TotalOperDELEGPURGE (7)	INTEGER	Statistics (%) for DELEGPURGE operations
7.8	nfsV4TotalOperDELEGRETURN (8)	INTEGER	Statistics (%) for DELEGRETURN operations
7.9	nfsV4TotalOperGETATTR (9)	INTEGER	Statistics (%) for GETATTR operations
7.10	nfsV4TotalOperGETFH (10)	INTEGER	Statistics (%) for GETFH operations
7.11	nfsV4TotalOperLINK (11)	INTEGER	Statistics (%) for LINK operations
7.12	nfsV4TotalOperLOCK (12)	INTEGER	Statistics (%) for LOCK operations
7.13	nfsV4TotalOperLOCKT (13)	INTEGER	Statistics (%) for LOCKT operations

ID	Object name	Type	Meaning
7.14	nfsV4TotalOperLOCKU (14)	INTEGER	Statistics (%) for LOCKU operations
7.15	nfsV4TotalOperLOOKUP (15)	INTEGER	Statistics (%) for LOOKUP operations
7.16	nfsV4TotalOperLOOKUPROOT (16)	INTEGER	Statistics (%) for LOOKUPROOT operations
7.17	nfsV4TotalOperNVERIFY (17)	INTEGER	Statistics (%) for NVERIFY operations
7.18	nfsV4TotalOperOPEN (18)	INTEGER	Statistics (%) for OPEN operations
7.19	nfsV4TotalOperOPENATTR (19)	INTEGER	Statistics (%) for OPENATTR operations
7.20	nfsV4TotalOperOPENCONF (20)	INTEGER	Statistics (%) for OPENCONF operations
7.21	nfsV4TotalOperOPENDGRD (21)	INTEGER	Statistics (%) for OPENDGRD operations
7.22	nfsV4TotalOperPUTFH (22)	INTEGER	Statistics (%) for PUTFH operations
7.23	nfsV4TotalOperPUTPUBFH (23)	INTEGER	Statistics (%) for PUTPUBFH operations
7.24	nfsV4TotalOperPUTROOTFH (24)	INTEGER	Statistics (%) for PUTROOTFH operations
7.25	nfsV4TotalOperREAD (25)	INTEGER	Statistics (%) for READ operations
7.26	nfsV4TotalOperREADDIR (26)	INTEGER	Statistics (%) for READDIR operations
7.27	nfsV4TotalOperREADLINK (27)	INTEGER	Statistics (%) for READLINK operations
7.28	nfsV4TotalOperREMOVE (28)	INTEGER	Statistics (%) for REMOVE operations
7.29	nfsV4TotalOperRENAME (29)	INTEGER	Statistics (%) for RENAME operations
7.30	nfsV4TotalOperRENEW (30)	INTEGER	Statistics (%) for RENEW operations
7.31	nfsV4TotalOperRESTOREFH (31)	INTEGER	Statistics (%) for RESTOREFH operations
7.32	nfsV4TotalOperSAVEFH (32)	INTEGER	Statistics (%) for SAVEFH operations
7.33	nfsV4TotalOperSECINFO (33)	INTEGER	Statistics (%) for SECINFO operations
7.34	nfsV4TotalOperSETATTR (34)	INTEGER	Statistics (%) for SETATTR operations
7.35	nfsV4TotalOperSETCLTID (35)	INTEGER	Statistics (%) for SETCLTID operations

ID	Object name	Type	Meaning
7.36	nfsV4TotalOperSETCLTIDCONF (36)	INTEGER	Statistics (%) for SETCLTIDCONF operations
7.37	nfsV4TotalOperVERIFY (37)	INTEGER	Statistics (%) for VERIFY operations
7.38	nfsV4TotalOperWRITE (38)	INTEGER	Statistics (%) for WRITE operations
7.39	nfsV4TotalOperRELOCKOWNER (39)	INTEGER	Statistics (%) for RELOCKOWNER operations

Table F-28 stdExMibCifs (5) group

ID	Object name	Type	Meaning
1	stdExMibCifsItem (1)	-	CIFS item
1.1	cifsWorkGroup (1)	DisplayString	Workgroup name
1.2	cifsSeverComment (2)	DisplayString	Server comment ^{#1}
1.3	cifsSecurity (3)	DisplayString	Authentication mode
1.4	cifsPasswordServer (4)	DisplayString	Authentication server ^{#1}
1.5	cifsSharesCount (5)	INTEGER	The number of current CIFS shares
1.6	cifsSessionCount (6)	Counter32	The number of current sessions ^{#2}
<p>^{#1}: No more than 255 characters are displayed, and the 256th and subsequent characters are truncated.</p> <p>^{#2}: The CIFS sessions established by specifying a NetBIOS name and those established by specifying an IP address are counted separately even when the sessions are established concurrently from the same client.</p>			

Table F-29 stdExMibNetwork (6) group

ID	Object name	Type	Meaning
1	stdExMibIPAddressTable (1)	-	IP address management
1.1	ipAddressEntry (1) ^{#1}	-	Details about each IP address
1.1.1	ipAddressIFIndex (1)	Integer32	Index number for each network interface
1.1.2	ipAddressAddr (2) ^{#2}	IpAddress	IP address
1.1.3	ipAddressIFName (3)	DisplayString	Network interface name
1.1.4	ipv6IpAddressAddr (4)	DisplayString	IP address (IPv6)
2	stdExMibDefaultGateway (2)	IpAddress	Default gateway

ID	Object name	Type	Meaning
3	stdExMibLinkAggregationGroup Table (3)	-	Trunking group information
3.1	lagEntry (1)	-	Trunking group entry
3.1.1	lagIndex (1)	Integer32	Trunking group index
3.1.2	lagMasterDeviceName (2)	DisplayString	Master device interface name for the trunking group
3.1.3	lagIpAddress (3)	IpAddress	Trunking group IP address
3.1.4	lagSubDeviceName (4)	DisplayString	Subdevice interface name for the trunking group
3.1.5	ipv6LagIpAddress (5)	DisplayString	Trunking group IP address (IPv6)
4	ipv6StdExMibDefaultGateway (4)	DisplayString	Default gateway (IPv6)
<p>#1: The IP address entries are output in the following order: <i>mng0</i>, <i>ethn</i>, <i>xgben</i>, and <i>pm0</i>. The maximum number of entries is <i>number-of-installed-ethn-and-xgben</i> + 3.</p> <p>#2: Acquisition of this MIB might fail because there is a standard MIB with the same name. If acquisition fails, specify the following: iso.org.dod.internet.private.enterprises.hitachi.systemExMib.storageExMib.stdExMib.stdExMibRAID.stdExMibRoot.stdExMibNetwork.stdExMibIPAddressTable.ipAddressEntry.ipAddressAddr</p>			

Table F-30 stdExMibPerformManager (7) group

ID	Object name	Type	Meaning
1	stdExMibNWPerformManagerTable (1)	-	Network performance monitoring
1.1	netWorkPmEntry (1)	-	Network performance monitoring for each interface
1.1.1	nwpmIFIndex (1)	Integer32	Index number for each network interface
1.1.2	nwpmRcvPacket (2)	Counter32	(This object is no longer available.)
1.1.3	nwpmSendPacket (3)	Counter32	(This object is no longer available.)
1.1.4	nwpmCollision (4)	Counter32	The number of collisions
1.1.5	nwpmBuffErrRcvPacket (5)	Counter32	The number of received packets that were discarded because of buffer insufficiency
1.1.6	nwpmBuffErrSendPacket (6)	Counter32	(This object is no longer available.)
1.1.7	nwpmPacketSendCareerErr (7)	Counter32	The number of career errors that occurred when sending packets

ID	Object name	Type	Meaning
1.1.8	nwpmFrmAlignmentErr (8)	Counter32	The number of frame alignment errors
1.1.9	nwpmFIFOSendOverRunErr (9)	Counter32	(This object is no longer available.)
1.1.10	nwpmFIFORcvOverRunErr (10)	Counter32	The number of FIFO overrun errors (receiving)
2	stdExMibLagPerformManagerTable (2)	-	Performance monitoring information for the trunking group
2.1	lagPerformManagerEntry (1)	-	Performance monitoring entry for the trunking group
2.1.1	lagpmIFIndex (1)	Integer32	Trunking group interface index
2.1.2	lagpmRcvPacket (2)	Counter32	Number of received compressed packets for the trunking group
2.1.3	lagpmSendPacket (3)	Counter32	Number of sent compressed packets for the trunking group
2.1.4	lagpmCollision (4)	Counter32	Number of times a collision occurred for the trunking group
2.1.5	lagpmBuffErrRcvPacket (5)	Counter32	Number of received packets discarded because of an insufficiency for the trunking group buffer
2.1.6	lagpmBuffErrSendPacket (6)	Counter32	Number of sent packets discarded because of an insufficiency for the trunking group buffer
2.1.7	lagpmPacketSendCareerErr (7)	Counter32	Number of carrier errors that occurred during sending of trunking group packets
2.1.8	lagpmFrmAlignmentErr (8)	Counter32	Number of frame alignment errors for the trunking group
2.1.9	lagpmFIFOSendOverRunErr (9)	Counter32	Number of FIFO overrun errors for the trunking group (during sending)
2.1.10	lagpmFIFORcvOverRunErr (10)	Counter32	Number of FIFO overrun errors for the trunking group (during receiving)

Table F-31 stdExMibFileSystem (11) group

ID	Object name	Type	Meaning
1	fileSystemTable (1)	-	File systems management
1.1	fileSystemEntry (1)	-	Management information for each file system

ID	Object name	Type	Meaning
1.1.1	fileSystemIndex (1)	Integer32	Index
1.1.2	fileSystemName (2)	DisplayString	File system path
1.1.3	fileSystemTotalCapacity (3)	Counter32	File system total capacity (MB)
1.1.4	fileSystemDeviceStatus (4)	INTEGER	LU status of the internal hard disk drive or storage system. Each value represents the following: 0: normal, 1: error
1.1.5	fileSystemKBCapacity (5)	Counter64	File system block capacity (KB)
1.1.6	fileSystemMBCapacity (6)	Counter64	File system block capacity (MB)
1.1.7	fileSystemGBCapacity (7)	Counter64	File system block capacity (GB)
1.1.8	fileSystemKBUsed (8)	Counter64	File system block usage (KB)
1.1.9	fileSystemMBUsed (9)	Counter64	File system block usage (MB)
1.1.10	fileSystemGBUsed (10)	Counter64	File system block usage (GB)
1.1.11	fileSystemUsedPercent (11)	INTEGER	File system usage rate (%)
1.1.12	fileSystemKBAvail (12)	Counter64	File system unused capacity (KB)
1.1.13	fileSystemMBAvail (13)	Counter64	File system unused capacity (MB)
1.1.14	fileSystemGBAvail (14)	Counter64	File system unused capacity (GB)
1.1.15	fileSystemInodeUsed (15)	Counter64	Number of used inodes
1.1.16	fileSystemInodeFree (16)	Counter64	Number of unused inodes
1.1.17	fileSystemMaxUsedInode (17)	INTEGER	Maximum percentage of the total capacity that can be used by inodes (%)
1.1.18	fileSystemVolumeManager (18)	INTEGER	Whether a volume manager can be used Each value represents the following: 0: --, 1: use
1.1.19	fileSystemMountStatus (19)	INTEGER	Mount status Each value represents the following: 0: ro, 1: rw, 2: --, 3: fatal error, 4: overflow, 5: not available, 6: blocked, 7: blocked and ready, 8: expanding, 9: reclaim
1.1.20	fileSystemTiering (20)	INTEGER	Whether tiers can be used Each value represents the following:

ID	Object name	Type	Meaning
			0: --, 1: use
2	fileSystemLUInfoTable (2)	-	Information about the LUs that make up the file system.
2.1	fileSystemLUInfoEntry (1)	-	Information about an LU that makes up the file system.
2.1.1	fileSystemLUInfoIndex (1)	Integer32	Index
2.1.2	fileSystemLUInfoDevice (2)	DisplayString	Name of the LU that makes up the file system.
2.1.3	fileSystemLUInfoFSName (3)	DisplayString	File system name
2.1.4	fileSystemLUInfoDeviceInfo (4)	INTEGER	Storage device information Each value represents the following: 0: P-vol, 1: D-vol
2.1.5	fileSystemLUInfoSerial (5)	DisplayString	Serial number
2.1.6	fileSystemLUInfoDataPool (6)	DisplayString	DP number for a data pool that makes up the file system

Table F-32 stdExMibHDPPool (12) group

ID	Object name	Type	Meaning
1	hdpPoolTable (1)	-	Pool management information
1.1	hdpPoolEntry (1)	-	Management information for each pool
1.1.1	hdpPoolIndex (1)	Integer32	Index
1.1.2	hdpPoolNumber (2)	DisplayString	Pool number
1.1.3	hdpPoolSerialNumber (3)	DisplayString	Serial number
1.1.4	hdpPoolDrive (4)	INTEGER	Drive type Each value represents the following: 0: FC/SAS, 1: SATA, 2: SSD, 3: SAS7K, 99: -
1.1.5	hdpPoolTotal (5)	Counter32	Total pool capacity (GB)
1.1.6	hdpPoolUsed (6)	Counter32	Used pool capacity (GB)
1.1.7	hdpPoolFree (7)	Counter32	Unused pool capacity (GB)
1.1.8	hdpPoolUsedPercent (8)	INTEGER	Pool usage rate (%)
1.1.9	hdpPoolEarlyAlertPercent (9)	INTEGER	Warning threshold (%)

ID	Object name	Type	Meaning
1.1.10	hdpPoolDepletionAlertPercent (10)	INTEGER	Critical threshold (%)
1.1.11	hdpPoolPvolFileSystemName (11)	OCTET STRING	File systems used by the pool

MIB objects used for SNMP traps

The following table lists the groups of MIB objects in the HDI system used for SNMP traps and the tables to be referenced for each group.

Table F-33 Groups of MIB objects used in SNMP traps and tables to be referenced

Group name	Description	Tables
stdExMibQuotaTrapFS (3)	A group related to quota monitoring.	Table F-34 stdExMibQuotaTrapFS (3) group on page F-68
stdExMibEvent (8)	A group related to event monitoring.	Table F-35 stdExMibEvent (8) group on page F-76

Tables [Table F-34 stdExMibQuotaTrapFS \(3\) group on page F-68](#) and [Table F-35 stdExMibEvent \(8\) group on page F-76](#) summarize the groups of MIB objects used in SNMP traps.

Table F-34 stdExMibQuotaTrapFS (3) group

ID	Object name	Type	Meaning
1	quotaTrapFSSoftLimitTable (1)	-	Information about traps that exceeded the soft limit
1.1	quotaSoftLimitEntry (1)	-	Details about traps that exceeded the soft limit
1.1.1	quotaSoftLimitTrapDate (1)	DisplayString	Time of trap occurrence
1.1.2	quotaSoftLimitCHAName (2)	DisplayString	Node host name
1.1.3	quotaSoftLimitCHANumber (3)	DisplayString	Node number
1.1.4	quotaSoftLimitRaidNumber (4)	DisplayString	Device ID
1.1.5	quotaSoftLimitFSMntPoint (5)	DisplayString	File system name
1.1.6	quotaSoftLimitType (6)	INTEGER	Difference between user quotas and group quotas Each value represents the following:

ID	Object name	Type	Meaning
			1: user, 2: group
1.1.7	quotaSoftLimitName (7)	DisplayString	User name or group name
1.1.8	quotaSoftLimitID (8)	Integer32	UID or GID
1.1.9	quotaSoftLimitClass (9)	INTEGER	Excess type (blocks or inodes) Each value represents the following: 1: block, 2: inode
1.1.10	quotaSoftLimitUsed (10)	Counter64	Current usage (if the excess type is blocks, the unit is KB)
1.1.11	quotaSoftLimitSoftLimitValue (11)	Counter64	Soft limit (if the excess type is blocks, the unit is KB)
1.1.12	quotaSoftLimitHardLimitValue (12)	Counter64	Hard limit (if the excess type is blocks, the unit is KB)
1.1.13	quotaSoftLimitRemainGracePeriod (13)	Counter32	Time (seconds) remaining for the grace period
2	quotaTrapFSLimitExceeded (2)	-	Information about traps that exceeded the grace period
2.1	quotaLimitExceededEntry (1)	-	Details about traps that exceeded the grace period
2.1.1	quotaLimitExceededTrapDate (1)	DisplayString	Time of trap occurrence
2.1.2	quotaLimitExceededCHAName (2)	DisplayString	Node host name
2.1.3	quotaLimitExceededCHANumber (3)	DisplayString	Node number
2.1.4	quotaLimitExceededRaidNumber (4)	DisplayString	Device ID
2.1.5	quotaLimitExceededFSMntPoint (5)	DisplayString	File system name
2.1.6	quotaLimitExceededType (6)	INTEGER	Difference between user quotas and group quotas Each value represents the following: 1: user, 2: group
2.1.7	quotaLimitExceededName (7)	DisplayString	User name or group name
2.1.8	quotaLimitExceededID (8)	Integer32	UID or GID
2.1.9	quotaLimitExceededClass (9)	INTEGER	Excess type (blocks or inodes) Each value represents the following: 1: block, 2: inode

ID	Object name	Type	Meaning
2.1.10	quotaLimitExceededUsed (10)	Counter64	Current usage (if the excess type is blocks, the unit is KB)
2.1.11	quotaLimitExceededSoftLimitValue (11)	Counter64	Soft limit (if the excess type is blocks, the unit is KB)
2.1.12	quotaLimitExceededHardLimitValue (12)	Counter64	Hard limit (if the excess type is blocks, the unit is KB)
2.1.13	quotaLimitExceededGracePeriodValue (13)	Counter32	Set value (days) for the grace period
3	quotaTrapFSSummary (3)	-	Information in the summary trap for quotas
3.1	quotaSummaryEntry (1)	-	Details in the summary trap for quotas
3.1.1	quotaSummaryTrapDate (1)	DisplayString	Time when trap occurred
3.1.2	quotaSummaryCHAName (2)	DisplayString	Node host name
3.1.3	quotaSummaryCHANumber (3)	DisplayString	Node number
3.1.4	quotaSummaryRaidNumber (4)	DisplayString	Device ID
3.1.5	quotaSummaryFSMntPoint (5)	DisplayString	File system name
3.1.6	quotaSummaryBlockSoftLimitExceedingUsers (6)	Integer32	Number of users who exceed their block soft limit
3.1.7	quotaSummaryBlockSoftLimitExceedingGroups (7)	INTEGER	Number of groups that exceed their block soft limit
3.1.8	quotaSummaryBlockGracePeriodExpiredUsers (8)	INTEGER	Number of users whose block grace period has expired
3.1.9	quotaSummaryBlockGracePeriodExpiredGroups (9)	INTEGER	Number of groups whose block grace period has expired
3.1.10	quotaSummaryFileSoftLimitExceedingUsers (10)	INTEGER	Number of users who exceed their file soft limit
3.1.11	quotaSummaryFileSoftLimitExceedingGroups (11)	INTEGER	Number of groups that exceed their file soft limit
3.1.12	quotaSummaryFileGracePeriodExpiredUser (12)	INTEGER	Number of users whose file grace period has expired
3.1.13	quotaSummaryFileGracePeriodExpiredGroups (13)	INTEGER	Number of groups whose file grace period has expired
4	quotaTrapFSDetailSuppress (4)	-	Information in the trap for quotas when individual reports are suppressed
4.1	quotaDetailSuppressEntry (1)	-	Details in the trap for quotas when individual reports are suppressed

ID	Object name	Type	Meaning
4.1.1	quotaDetailSuppressTrapDate (1)	DisplayString	Time when trap occurred
4.1.2	quotaDetailSuppressCHAName (2)	DisplayString	Node host name
4.1.3	quotaDetailSuppressCHANumber (3)	DisplayString	Node number
4.1.4	quotaDetailSuppressRaidNumber (4)	DisplayString	Device ID
4.1.5	quotaDetailSuppressFSMntPoint (5)	DisplayString	File system name
4.1.6	quotaDetailSuppressType (6)	INTEGER	Difference between user quotas and group quotas Each value represents the following: 1: user, 2: group
4.1.7	quotaDetailSuppressBlockSoftLimitExceeding (7)	INTEGER	Number of users or groups that exceed their block soft limit
4.1.8	quotaDetailSuppressBlockGracePeriodExpired (8)	INTEGER	Number of users or groups whose block grace period has expired
4.1.9	quotaDetailSuppressFileSoftLimitExceeding (9)	INTEGER	Number of users or groups that exceed their file soft limit
4.1.10	quotaDetailSuppressFileGracePeriodExpired (10)	INTEGER	Number of users or groups whose file grace period has expired
5	quotaTrapFSSubtreeSoftLimitTable (5)	-	Information about traps that exceeded the soft limit for monitoring subtree quotas
5.1	quotaSubtreeSoftLimitEntry (1)	-	Details about traps that exceeded the soft limit for monitoring subtree quotas
5.1.1	quotaSubtreeSoftLimitTrapDate (1)	DisplayString	Time of trap occurrence
5.1.2	quotaSubtreeSoftLimitCHAName (2)	DisplayString	Node host name
5.1.3	quotaSubtreeSoftLimitCHANumber (3)	DisplayString	Node number
5.1.4	quotaSubtreeSoftLimitRaidNumber (4)	DisplayString	Device ID
5.1.5	quotaSubtreeSoftLimitFSDirName (5)	DisplayString	File system name/directory name
5.1.6	quotaSubtreeSoftLimitType (6)	INTEGER	Quota type: Subtree quota Each value represents the following: 2: subtree

ID	Object name	Type	Meaning
5.1.7	quotaSubtreeSoftLimitName (7)	DisplayString	NULL
5.1.8	quotaSubtreeSoftLimitID (8)	Integer32	-1
5.1.9	quotaSubtreeSoftLimitClass (9)	INTEGER	Excess type (blocks or inodes) Each value represents the following: 1: block, 2: inode
5.1.10	quotaSubtreeSoftLimitUsed (10)	Counter64	Current usage (if the excess type is blocks, the unit is KB)
5.1.11	quotaSubtreeSoftLimitSoftLimitValue (11)	Counter64	Soft limit (if the excess type is blocks, the unit is KB)
5.1.12	quotaSubtreeSoftLimitHardLimitValue (12)	Counter64	Hard limit (if the excess type is blocks, the unit is KB)
5.1.13	quotaSubtreeSoftLimitRemainingGracePeriod (13)	Counter32	Time (seconds) remaining for the grace period
6	quotaTrapFSSubtreeLimitExceeded (6)	-	Information about traps that exceeded the grace period for monitoring subtree quotas
6.1	quotaSubtreeLimitExceededEntry (1)	-	Details about traps that exceeded the grace period for monitoring subtree quotas
6.1.1	quotaSubtreeLimitExceededTrapDate (1)	DisplayString	Time of trap occurrence
6.1.2	quotaSubtreeLimitExceededCHAName (2)	DisplayString	Node host name
6.1.3	quotaSubtreeLimitExceededCHANumber (3)	DisplayString	Node number
6.1.4	quotaSubtreeLimitExceededRaidNumber (4)	DisplayString	Device ID
6.1.5	quotaSubtreeLimitExceededFSDirName (5)	DisplayString	File system name/directory name
6.1.6	quotaSubtreeLimitExceededType (6)	INTEGER	Quota type: Subtree quota Each value represents the following: 2: subtree
6.1.7	quotaSubtreeLimitExceededName (7)	DisplayString	NULL
6.1.8	quotaSubtreeLimitExceededID (8)	Integer32	-1
6.1.9	quotaSubtreeLimitExceededClass (9)	INTEGER	Excess type (blocks or inodes) Each value represents the following: 1: block, 2: inode

ID	Object name	Type	Meaning
6.1.10	quotaSubtreeLimitExceededUsed (10)	Counter64	Current usage (if the excess type is blocks, the unit is KB)
6.1.11	quotaSubtreeLimitExceededSoftLimitValue (11)	Counter64	Soft limit (if the excess type is blocks, the unit is KB)
6.1.12	quotaSubtreeLimitExceededHardLimitValue (12)	Counter64	Hard limit (if the excess type is blocks, the unit is KB)
6.1.13	quotaSubtreeLimitExceededGracePeriodValue (13)	Counter32	Set value (days) for the grace period
7	quotaTrapFSSubtreeSummary (7)	-	Information in the summary trap for subtree quotas
7.1	quotaSubtreeSummaryEntry (1)	-	Details in the summary trap for subtree quotas
7.1.1	quotaSubtreeSummaryTrapDate (1)	DisplayString	Time when trap occurred
7.1.2	quotaSubtreeSummaryCHAName (2)	DisplayString	Node host name
7.1.3	quotaSubtreeSummaryCHANumber (3)	DisplayString	Node number
7.1.4	quotaSubtreeSummaryRaidNumber (4)	DisplayString	Device ID
7.1.5	quotaSubtreeSummaryFSDirName (5)	DisplayString	File system name or file system name/directory name
7.1.6	quotaSubtreeSummaryType (6)	INTEGER	Summary type: Subtree quota or subtree user group quota Each value represents the following: 2: subtree, 5: subtree-user-group
7.1.7	quotaSubtreeSummaryBlockSoftLimitExceedingUsers (7)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of users who exceed their soft limit for the number of blocks.
7.1.8	quotaSubtreeSummaryBlockSoftLimitExceedingGroups (8)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of groups that exceed their soft limit for the number of blocks.
7.1.9	quotaSubtreeSummaryBlockSoftLimitExceedingDirectories (9)	INTEGER	If the summary type is subtree quota, this value is the number of directories that exceed their soft limit for the number of blocks.

ID	Object name	Type	Meaning
			If the summary type is subtree user group quota, this value is -1.
7.1.10	quotaSubtreeSummaryBlockGracePeriodExpiredUsers (10)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of users whose grace period for the number of blocks has expired.
7.1.11	quotaSubtreeSummaryBlockGracePeriodExpiredGroups (11)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of groups whose grace period for the number of blocks has expired.
7.1.12	quotaSubtreeSummaryBlockGracePeriodExpiredDirectories (12)	INTEGER	If the summary type is subtree quota, this value is the number of directories whose grace period for the number of blocks has expired. If the summary type is subtree user group quota, this value is -1.
7.1.13	quotaSubtreeSummaryFileSoftLimitExceedingUsers (13)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of users who exceed their soft limit for the number of inodes.
7.1.14	quotaSubtreeSummaryFileSoftLimitExceedingGroups (14)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of groups that exceed their soft limit for the number of inodes.
7.1.15	quotaSubtreeSummaryFileSoftLimitExceedingDirectories (15)	INTEGER	If the summary type is subtree quota, this value is the number of directories that exceed their soft limit for the number of inodes. If the summary type is subtree user group quota, this value is -1.
7.1.16	quotaSubtreeSummaryFileGracePeriodExpiredUsers (16)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of users whose grace period for the number of inodes has expired.

ID	Object name	Type	Meaning
7.1.17	quotaSubtreeSummaryFileGracePeriodExpiredGroups (17)	INTEGER	If the summary type is subtree quota, this value is -1. If the summary type is subtree user group quota, this value is the number of groups whose grace period for the number of inodes has expired.
7.1.18	quotaSubtreeSummaryFileGracePeriodExpiredDirectories (18)	INTEGER	If the summary type is subtree quota, this value is the number of directories whose grace period for the number of inodes has expired. If the summary type is subtree user group quota, this value is -1.
8	quotaTrapFSSubtreeDetailSuppress (8)	-	Information in the trap for subtree quotas when individual reports are suppressed
8.1	quotaSubtreeDetailSuppress Entry (1)	-	Details in the trap for subtree quotas when individual reports are suppressed
8.1.1	quotaSubtreeDetailSuppress TrapDate (1)	DisplayString	Time when trap occurred
8.1.2	quotaSubtreeDetailSuppress CHAName (2)	DisplayString	Node host name
8.1.3	quotaSubtreeDetailSuppress CHANumber (3)	DisplayString	Node number
8.1.4	quotaSubtreeDetailSuppress RaidNumber (4)	DisplayString	Device ID
8.1.5	quotaSubtreeDetailSuppress FSDirName (5)	DisplayString	File system name/directory name
8.1.6	quotaSubtreeDetailSuppress Type (6)	INTEGER	Quota type: Subtree quota Each value represents the following: 2: subtree
8.1.7	quotaSubtreeDetailSuppress BlockSoftLimitExceeding (7)	INTEGER	Number of directories that exceed their soft limit for the number of blocks
8.1.8	quotaSubtreeDetailSuppress BlockGracePeriodExpired (8)	INTEGER	Number of directories whose grace period for the number of blocks has expired
8.1.9	quotaSubtreeDetailSuppress FileSoftLimitExceeding (9)	INTEGER	Number of directories that exceed their soft limit for the number of inodes
8.1.10	quotaSubtreeDetailSuppress FileGracePeriodExpired (10)	INTEGER	Number of directories whose grace period for the number of inodes has expired



Tip: For details about how to use subtree quotas, see the *CLI Administrator's Guide*.

Table F-35 stdExMibEvent (8) group

ID	Object name	Type	Meaning
1	stdExMibEventTrap (1)	-	Information about event notification traps
1.1	eventTrapEntry (1)	-	Details about event notification traps
1.1.1	eventTrapDate (1)	DisplayString	Time of trap occurrence
1.1.2	eventTrapGenDate (2)	DisplayString	Time of event occurrence
1.1.3	eventTrapCHAName (3)	DisplayString	Node host name
1.1.4	eventTrapCHANumber (4)	DisplayString	Node number
1.1.5	eventRaidNumber (5)	DisplayString	Device ID
1.1.6	eventTrapProcessID (6)	Integer32	Process ID
1.1.7	eventTrapProcessName (7)	DisplayString	Process name
1.1.8	eventTrapMsgID (8)	DisplayString	Message ID
1.1.9	eventTrapMsg (9)	OCTET STRING	Event message
1.1.10	eventTrapImportanceDeg (10)	Counter32	Importance level
1.1.11	eventTrapSameCount (11)	Counter32	The number of times that the same event occurred
1.1.12	eventTrapFinalGenerationDate (12)	DisplayString	Time of last occurrence
1.1.13	eventTrapThreadFlag (13)	INTEGER	Event flag
1.2	eventTrapOption (2)	-	Additional event information trap
1.2.1	eventTrapOptionFSName (1)	DisplayString	File system name
1.2.2	eventTrapOptionMntPoint (2)	DisplayString	Mount point
1.2.3	eventTrapOptionFileCount (3)	Counter64	Number of files (inodes)
1.2.4	eventTrapOptionFileWarnThld (4)	Counter64	Warning threshold (number of inodes)
1.2.5	eventTrapOptionAvail (5)	Counter64	Unused capacity (KB)
1.2.6	eventTrapOptionAvailWarnThld (6)	Counter64	Warning threshold (KB)
1.2.7	eventTrapOptionFunction (7)	DisplayString	Function name
2	stdExMibCoreTrap (2)	-	Information about core notification traps
2.1	coreTrapEntry (1)	-	Details about core notification traps

ID	Object name	Type	Meaning
2.1.1	coreTrapTrapDate (1)	DisplayString	Time of trap occurrence
2.1.2	coreTrapCHAName (2)	DisplayString	Node host name
2.1.3	coreTrapCHANumber (3)	DisplayString	Node number
2.1.4	coreTrapRaidNumber (4)	DisplayString	Device ID
2.1.5	coreTrapGenerationDate (5)	DisplayString	Time of occurrence
2.1.6	coreTrapDirectoryFileName (6)	DisplayString	Directory name or file name
2.1.7	coreTrapSize (7)	Integer32	Size (bytes)
2.1.8	coreTrapSystemDiskFreeSpace (8)	INTEGER	Free space (MB) on the system disk
2.1.9	coreTrapSystemDiskUse (9)	INTEGER	Usage rate (%) of the system disk

There are 4 values (Information, Warning, Error, and Fatal Error) for the severity level (eventTrapImportanceDeg (10)) for the SNMP trap event that is sent by the MIB object for stdExMibEventTrap (1).

The following table shows the meanings and values for eventTrapImportanceDeg (10).

Table F-36 Severity level for the SNMP trap event

Severity level value (eventTrapImportanceDeg (10))	Meaning
0	Information
10	Warning
20	Error
30	Fatal Error

For each event, check the message ID (eventTrapMsgID (8)) and message (eventTrapMsg (9)), see the *Error Codes* manual, and then take appropriate action.

Also, for details about messages sent to the SNMP manager by SNMP trapping, see the *Error Codes* manual.



Operation reference information

This appendix explains reference information for running HDI systems consisting of a single node.

- [List of reference information](#)

List of reference information

The following gives the manuals to be referenced for reference information about running HDI systems.

Table G-1 List of reference information

Reference information	See
Maximum number of CIFS clients	<i>File System Protocols (CIFS/NFS) Administrator's Guide</i>
ACL types for file systems and available functionality	<i>Installation and Configuration Guide</i>
How to manage users	
Items to be checked when managing quota	
External servers and services available in IPv6	
Items to be checked when managing file shares	<i>Installation and Configuration Guide</i> <i>File System Protocols (CIFS/NFS) Administrator's Guide</i>
Lists of the commands provided in single-node configurations of HDI systems	<i>CLI Administrator's Guide</i>



Node maintenance

This appendix describes the maintenance that the system administrator must sometimes perform for an HDI system in a single-node configuration.

- [Starting and forcibly stopping a node OS](#)
- [Replacing the internal RAID battery](#)
- [Managing the RAID card](#)

Starting and forcibly stopping a node OS

This section explains how to control the node power for maintenance, by starting or forcibly stopping the OS.

Starting an OS

You can start an OS by using the power switch or power button to turn on the node.

To start the OS by turning on the power to a node:

1. Make sure that the external servers connected to the node are running.
2. Make sure that the power lamp, power LED or power indicator located on the front of the node is off.
3. If you use a storage system connected to the HDI system, make sure that the storage system and FC switch are running.
If you start the OS while the storage system and FC switch are not running, an error will occur on the FC path.
4. If encryption of local data is enabled, when you save system settings on the HCP system, confirm that the HCP system is running normally, and that the HDI and HCP systems can communicate normally.
User data cannot be available unless the HCP system can be communicated with.
5. Press the power switch or power button located on the front of the node.
6. Make sure that the power lamp, power LED or power indicator lights up.

Forcibly Stopping an OS

Normally, the CLI is used to stop the OS. However, if the power lamp, power LED or power indicator cannot be turned off via commands, you can shutdown the node to forcibly stop the OS. Follow the maintenance personnel's instructions when you shutdown the node.

To forcibly stop the OS by turning off the power to a node:

1. Hold down the power switch or power button located on the front of the node for 5 seconds or more.
2. Make sure that the power lamp, power LED or power indicator is off.

Replacing the internal RAID battery

Note: For models that do not use the internal RAID battery, this replacement operation is unnecessary.

The battery backup unit (BBU) for the RAID card is called the internal RAID battery. Because the internal RAID battery is expendable, we recommend that you replace the internal RAID battery once a year. Replacement parts are subject to fees. For details about how to replace the internal RAID battery, see documentation provided with the device.

If the internal RAID battery causes an error or becomes low on power, an event is both sent out via an SNMP trap or email and output to the log file. The system administrator must take action according to output messages (KAQG46509-I, KAQG46510-W).

Managing the RAID card

Note: For models that do not use the internal RAID battery, this management operation is unnecessary.

By using the `cachedbadbbuset` command, the system administrator can change the writing mode of the RAID card cache which is set when the internal RAID battery becomes low on power.

By default, when the internal RAID battery becomes low on power, the write mode of the RAID card cache is changed from `Write Back` to `Write Through`, and then the system performance decreases to protect data.

If you change the default setting so that `Write Back` mode is set even if the battery becomes low on power, the data that is not written into the internal hard disk might be lost when an error occurs, but `Write Back` mode can place priority on the system performance. You can check the specified write mode by using the `cachedbadbbuget` command.

Also, the internal RAID battery adjusts itself regularly by charging and discharging itself. The system administrator can use the `bbuschlset` command to set the date and time to charge and discharge the internal RAID battery. Review the settings for the write mode of the RAID card cache as necessary because the charge and discharge causes the battery power level to drop temporarily, which the system sees as the battery being low on power. The total time required for charge and discharge is about 12 hours. The operation time depends on the status of the internal RAID battery.



Terminology used in messages and related documents

This appendix describes the differences in terminology to be aware of when viewing the messages output by HDI and related documents.

- [Viewing messages and related documents](#)

Viewing messages and related documents

The messages output by HDI and some of the related documents are used for both HDI cluster configurations and single-node configurations. As such, terms used in the messages and documents might differ from the terms used for HDI single-node configurations, and functionality not used by HDI systems in single-node configurations might be listed in the messages and documents.

- When reading messages, replace the following terminology with the corresponding terminology used in single-node configurations of HDI systems.

Table I-1 Replacing the terminology used in cluster configurations of HDI systems

Terminology in messages	Terminology used in single-node configurations
Device file	LUs in the internal hard disk or storage system
Fixed IP address	IP address
System LU	System disk
User LU	User disk

- In explanations that refer to clusters, nodes, and resource groups, only the explanations pertaining to resource groups apply.
- Ignore any explanations regarding virtual IP addresses, heartbeat ports, failovers, and failbacks, because these terms are not used in single-node HDI systems.
- Cluster management LU refers to the drive capacity that has been allocated to store system settings information.



Acronyms

This appendix lists the acronyms used in the HDI manuals.

- [Acronyms used in the HDI manuals](#)

Acronyms used in the HDI manuals

The following acronyms are used in the HDI manuals.

ABE	Access Based Enumeration
ACE	access control entry
ACL	access control list
AES	Advanced Encryption Standard
AJP	Apache JServ Protocol
API	application programming interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BDC	Backup Domain Controller
BMC	baseboard management controller
CA	certificate authority
CHA	channel adapter
CHAP	Challenge-Handshake Authentication Protocol
CIFS	Common Internet File System
CIM	Common Information Model
CLI	command line interface
CPU	central processing unit
CSR	certificate signing request
CSV	comma-separated values
CTL	controller
CU	control unit
CV	custom volume
DACL	discretionary access control list
DAR	Direct Access Recovery
DB	database
DBMS	database management system
DC	domain controller
DDNS	Dynamic Domain Name System
DEP	data execution prevention
DES	Data Encryption Standard
DFS	distributed file system
DHCP	Dynamic Host Configuration Protocol

DIMM	dual in-line memory module
DLL	dynamic-link library
DN	distinguished name
DNS	Domain Name System
DOM	Document Object Model
DOS	Disk Operating System
DRAM	dynamic random access memory
DSA	digital signal algorithm
DTD	Document Type Definition
ECC	error-correcting code
EUC	Extended UNIX Code
FC	Fibre Channel
FC-SP	Fibre Channel - Security Protocol
FIB	forwarding information base
FIFO	First In, First Out
FQDN	fully qualified domain name
FTP	File Transfer Protocol
FV	Fixed Volume
FXP	File Exchange Protocol
GbE	Gigabit Ethernet
GID	group identifier
GMT	Greenwich Mean Time
GPL	GNU General Public License
GUI	graphical user interface
HBA	host bus adapter
H-LUN	host logical unit number
HPFS	High Performance File System
HSSO	HiCommand single sign-on
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	input/output
ICAP	Internet Content Adaptation Protocol
ICMP	Internet Control Message Protocol
ID	identifier

IP	Internet Protocol
IP-SW	IP switch
JDK	Java Development Kit
JIS	Japanese Industrial Standards
JSP	JavaServer Pages
KDC	Key Distribution Center
LACP	Link Aggregation Control Protocol
LAN	local area network
LBA	logical block addressing
LCD	Local Configuration Datastore
LDAP	Lightweight Directory Access Protocol
LDEV	logical device
LDIF	LDAP Data Interchange Format
LDKC	logical disk controller
LED	light-emitting diode
LF	Line Feed
LTS	long term support
LU	logical unit
LUN	logical unit number
LUSE	logical unit size expansion
LVI	Logical Volume Image
LVM	Logical Volume Manager
MAC	Media Access Control
MD5	Message-Digest algorithm 5
MIB	management information base
MMC	Microsoft Management Console
MP	microprocessor
MSS	maximum segment size
MTU	maximum transmission unit
NAS	Network-Attached Storage
NAT	network address translation
NDMP	Network Data Management Protocol
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIC	network interface card

NIS	Network Information Service
NTFS	New Technology File System
NTP	Network Time Protocol
OID	object identifier
ORB	object request broker
OS	operating system
PAP	Password Authentication Protocol
PC	personal computer
PCI	Peripheral Component Interconnect
PDC	Primary Domain Controller
PDU	protocol data unit
PID	process identifier
POSIX	Portable Operating System Interface for UNIX
PP	program product
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RAM	random access memory
RAS	Reliability Availability Serviceability
RCS	Revision Control System
RD	relational database
RFC	Request for Comments
RID	relative identifier
RPC	remote procedure call
RSA	Rivest, Shamir, and Adleman
SACL	system access control list
SAN	storage area network
SAS	Serial Attached SCSI
SATA	serial ATA
SAX	Simple API for XML
SCSI	Small Computer System Interface
SFTP	SSH File Transfer Protocol
SHA	secure hash algorithm
SID	security identifier
SJIS	Shift JIS
SLPR	Storage Logical Partition

SMB	Server Message Block
SMD5	Salted Message Digest 5
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SP	service pack
SSD	solid-state drive
SSH	Secure Shell
SSHA	Salted Secure Hash Algorithm
SSL	Secure Sockets Layer
SSO	single sign-on
SVGA	Super Video Graphics Array
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOS	type of service
TTL	time to live
UAC	User Account Control
UDP	User Datagram Protocol
UID	user identifier
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UTF	UCS Transformation Format
VDEV	Virtual Device
VLAN	virtual LAN
VLL	Virtual LVI/LUN
WADL	Web Application Description Language
WAN	wide area network
WINS	Windows Internet Name Service
WORM	Write Once, Read Many
WS	workstation
WWN	World Wide Name

WWW	World Wide Web
XDR	External Data Representation
XFS	extended file system
XML	Extensible Markup Language



Glossary

This glossary explains the terms used in this manual.

A

ACE

An entry in an ACL. An ACE sets access permissions for directories and files for each user and group. ACE formats differ depending on the ACL type.

ACL

A list of all the ACEs for a particular directory or file. An ACL defines the access permissions for a particular directory or file.

ACL type

The type of file system or file that is supported by the ACL. The ACL types that can be used in HDI systems are the Advanced ACL type (compatible with NTFS ACL), and the Classic ACL type (compatible with POSIX ACL).

Anti-Virus Enabler

A program used to scan, in real time, for viruses in data shared with users via CIFS in an HDI system.

B

Backup Restore

A program used for backing up data in an HDI file system.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

C

CIFS

A protocol that provides file-sharing services to Windows users.

D

Data Control

One of the programs on a node OS.

Dynamic Provisioning

A function that virtually allocates volumes of a given capacity to a host independent of the physical capacity of the storage system.

Dynamic Tiering

This storage system functionality automatically reallocates data based on I/O load.

F

File Sharing

One of the programs on a node OS.

front-end LAN

A LAN used by a client to access data stored in an HDI system.

I

interface

A logical network interface assigned to a port.

M

maintenance personnel

Hitachi engineers who maintain HDI systems.

management console

A computer used by the system administrator to operate HDI.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

N

NFS

A protocol that provides file-sharing services to UNIX users.

O

OS disk

A logical disk area in a node, that stores the OS and programs that run on the OS.

P

Primary Server Base

A program that provides Web server functionality.

Q

quota

The maximum block space and maximum number of inodes available to a user. In an HDI system, quotas can be set and managed for each file system and directory.

R

resource group

A management unit used to manage multiple resources (such as NFS share settings, CIFS share settings, file system information, and IP address information) as a group.

S

system administrator

A user who manages an HDI system. The system administrator sets up an HDI system and monitors system operations and error information.

system disk

A disk in a node that contains HDI system settings and programs that run on the node.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

T

trunking

A technology used to create a virtual network interface from a group of ports. In an HDI system, you can create a network that comprises virtual network interfaces that were created by using this technology.

U

user disk

The user disk is made up of volume groups.

user mapping

The process of assigning a user ID and group ID to a user registered in a domain controller when the user accesses a CIFS share.

V

volume group

A volume group is used to manage disk areas in internal hard disks or storage systems where user data is stored. A specific part of the capacity of a volume group is allocated to a file system.

W

WORM

An abbreviation for "Write Once, Read Many". The WORM status indicates that data cannot be modified. A file whose status is changed to the WORM status is called a WORM file, and a file system in which any files can be changed to a WORM file is called a WORM file system.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

Index

A

- access
 - CIFS client logs 4-10
 - setting up environment for CIFS client 4-2
 - setting up environment for NFS client 4-11
- account
 - changing password 2-2
- Active Directory
 - joining domain 4-2
 - rejoining domain 4-5
- adding
 - routing information 9-4
- application area B-4
- automatic account lockout settings
 - changing (system administrator) 2-2

B

- backing up
 - system configuration regularly 8-2
 - system configuration, manually 8-2
 - tape device 7-2

C

- cache residency 3-5
- cascaded trunking 9-9
- changing
 - account password 2-2
 - disk use 6-4
 - negotiation mode 9-5
 - node host name 9-3
 - node IP address 9-2

- policy for migrating data to HCP 3-4
 - schedule for migrating data to HCP 3-4
- combining link aggregation and link alternation 9-9
- command
 - setting up environment 11-2
- configuring
 - workgroup 4-7
- creating
 - shared directory 3-2

D

- data
 - showing migrated to HCP 5-2
- deleting
 - routing information 9-4
 - volume group 6-4
 - volume group LUs 6-4
- disks
 - changing use 6-4

E

- end user
 - GUI operation D-1
- error email notifications 10-6
- expanding capacity
 - file systems 3-6
- expansion
 - increasing the number of disks 6-2

F

- file server
 - importation from 3-6
- file systems
 - expanding capacity 3-6

G

- global tab area B-3
- global taskbar area B-2
- groups of MIB objects F-3
- GUI
 - basic operations B-1
 - notes on using B-5
 - operation by end user D-1
 - operations A-1
 - reference C-1
 - window configurations B-2

H

- HCP
 - changing migration policy 3-4
 - changing migration schedule 3-4
 - showing previous data 5-2
- host name
 - changing for node 9-3

I

- identifying
 - users by user mapping 4-9
- importation
 - file server 3-6
- increasing
 - number of disks 6-2
- IP address
 - changing for node 9-2

J

- joining
 - Active Directory domain 4-2
 - NT domain 4-5

L

- link aggregation 9-7
 - combining with link alternation 9-9
- link alternation 9-8
 - combining with link aggregation 9-9
 - performing manually 9-10
- logging on 1-2
- LUs
 - deleting from volume groups 6-4

M

- maintenance
 - node H-1
- MIB object F-1
 - responding to SNMP get request F-3
 - used for SNMP trap F-68
- migration
 - changing policy 3-4
 - changing schedule 3-4

N

- navigation area B-3
- negotiation mode
 - changing 9-5
- node
 - maintenance H-1
- NT domain
 - joining 4-5
- number of disks
 - increasing 6-2

O

- OS
 - forcibly stopping H-2
 - starting H-2

P

- password policy
 - changing (system administrator) 2-2
- policy
 - changing for migrating data to HCP 3-4
- power indicator H-2
- power lamp H-2

R

- reference
 - other HDI data 3-3
- rejoining
 - Active Directory domain 4-5
- reserved words E-1
- restoring
 - tape device 7-4
- RID 4-9
- routing information
 - adding 9-4
 - deleting 9-4

S

- schedule
 - changing for migrating data to HCP 3-4
- session timeout
 - changing (system administrator) 2-2
- setting
 - conditions for preventing files from turning into stub files 3-5
 - link aggregation 9-7
 - link alternation 9-8
- setting up
 - access environment from CIFS client 4-2
 - access environment from NFS client 4-11
 - environment for command 11-2
 - link configuration 9-7
 - public key certificate 11-2
 - virus scanning 7-2
 - VLAN 9-10
- shared directory
 - creating 3-2
- showing
 - previous data migrated to HCP 5-2
- SNMPv2
 - using 10-2
- SNMPv3
 - using 10-3
- software
 - updating 12-2
- structure for standard MIB objects F-2
- stub files
 - setting exceptions 3-5
- system administrator
 - automatic account lockout settings 2-2
 - password policy 2-2

- session timeout 2-2
- system configuration
 - backing up manually 8-2
 - backing up regularly 8-2

T

- tape device
 - backing up data 7-2
 - restoring data 7-4

U

- updating
 - software 12-2
 - using installation file registered in HCP system 12-2
 - using installation media 12-3
- user mapping 4-9
- using
 - SNMPv2 10-2
 - SNMPv3 10-3

V

- virus scanning setup 7-2
- VLAN ID 9-10
- VLAN setup 9-10
- volume group
 - deleting 6-4

W

- workgroup
 - configuring 4-7

Hitachi Vantara

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HitachiVantara.co
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

