



Hitachi HiCommand® Device Manager Server Installation and Configuration Guide

Notice: 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 any purpose, without the express written permission of Hitachi Data Systems Corporation (herein referred to as "Hitachi Data Systems").

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi Data Systems products and services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements. All of the features described in this document may not be currently available. See the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

Trademarks

Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., and the Hitachi Data Systems design mark is a trademark and service mark of Hitachi, Ltd.

HiCommand is a registered trademark of Hitachi, Ltd.

Hitachi Lightning 9900, ShadowImage, TagmaStore, Thunder 9200, Thunder 9500, and TrueCopy are trademarks of Hitachi Data Systems Corporation.

Borland, InterBase, and InterClient are registered trademarks of Borland Software Corporation.

AIX is a registered trademark of International Business Machines (IBM).

Pentium is a registered trademark of Intel Corporation.

JavaScript is a trademark or a registered trademark of Sun Microsystems, Inc. in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, and Windows NT are registered trademarks and Windows Server is a trademark of Microsoft Corporation.

Mozilla is a trademark of the Mozilla Organization.

Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries.

OS/390 is a trademark of the International Business Machines Corp. in the U.S.

RSA is a registered trademark of RSA Security, Inc.

Java, JavaScript, Solaris, Sun, and Sun StorEdge are trademarks of Sun Microsystems, Inc.

SPARC is a registered trademark of SPARC International, Inc. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

VERITAS is a trademark or registered trademark of Symantec Corporation in the U.S. and other countries.

Win32 is a registered trademark of Microsoft Corp. in the U.S. and other countries.

VMware and ESX Server are trademarks of VMware, Inc.

InstallAnywhere is a registered trademark of Zero G Software, Inc.

z/OS is a registered trademark of International Business Machines Corp. in the U.S.

All other brand or product names are or may be registered trademarks, trademarks or service marks of and are used to identify products or services of their respective owners.

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Data Systems Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK-91HC002-00	September 2001	Initial Release
MK-91HC002-01	October 2001	Revision 1, supersedes and replaces MK-91HC002-00
MK-91HC002-02	November 2001	Revision 2, supersedes and replaces MK-91HC002-01
MK-91HC002-03	January 2002	Revision 3, supersedes and replaces MK-91HC002-02
MK-91HC002-04	February 2002	Revision 4, supersedes and replaces MK-91HC002-03
MK-91HC002-05	June 2002	Revision 5, supersedes and replaces MK-91HC002-04
MK-91HC002-06	November 2002	Revision 6, supersedes and replaces MK-91HC002-05
MK-91HC002-07	May 2003	Revision 7, supersedes and replaces MK-91HC002-06
MK-91HC002-08	July 2003	Revision 8, supersedes and replaces MK-91HC002-07
MK-91HC002-09	September 2003	Revision 9, supersedes and replaces MK-91HC002-08
MK-91HC002-10	February 2004	Revision 10, supersedes and replaces MK-91HC002-09
MK-91HC002-11	April 2004	Revision 11, supersedes and replaces MK-91HC002-10
MK-91HC002-12	August 2004	Revision 12, supersedes and replaces MK-91HC002-11
MK-91HC002-13	October 2004	Revision 13, supersedes and replaces MK-91HC002-12

MK-91HC002-14P	March 2005	Preliminary release of Revision 14, supersedes and replaces MK-91HC002-13
MK-91HC002-14	June 2005	Revision 14, supersedes and replaces MK-91HC002-14P
MK-91HC002-15	July 2005	Revision 15, supersedes and replaces MK-91HC002-14
MK-91HC002-16	September 2005	Revision 16, supersedes and replaces MK-91HC002-15
MK-91HC002-17	February 2006	Revision 17, supersedes and replaces MK-91HC002-16
MK-91HC002-18	June 2006	Revision 18, supersedes and replaces MK-91HC002-17
MK-91HC002-19	November 2006	Revision 19, supersedes and replaces MK-91HC002-18

Source Document(s) for this Revision

- 3020-3-J73(E) dated November 30, 2005 (SD TI T-code document)
- 3020-3-J73(E) dated December 27, 2005 (SD TI T-code2 document)
- 3020-3-J73(E) dated January 31, 2006 (SD TI Q-code document)
- SSD-91HC002-R18b dated April 27, 2006 (SD TI Q-code document)

Preface

This document describes how to install and operate HiCommand Device Manager (hereafter abbreviated to Device Manager) and HiCommand Suite Common Component. It also includes troubleshooting for these program products.

This user's guide assumes that you as a user have basic knowledge of the following:

- Management tools appropriate to the individual storage subsystem
- Storage Area Networks (SANs)
- The Windows®, Solaris™, or Linux operating system required for Device Manager

Please contact your Hitachi Data Systems account team or see the Hitachi Data Systems worldwide web site (<http://www.hds.com>) for additional information on subsystem features and functions.

Notes:

- The use of the Sun StorEdge™ T3 Array and all other Sun™ products is governed by the terms of your agreement(s) with Sun Microsystems, Inc.
- This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).
- This product includes software developed by Borland® Software Corp. The interclient.jar file was developed by InterBase® Software Corp and its successors, and includes elements created by Borland/Inprise.
- This product includes software developed for use in the mod_ssl project (<http://www.modssl.org/>).
- The use of the HiCommand Device Manager products and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems and/or Sun™ Microsystems.

Release Notes

Applicable Release Notes can be found on the installation CD. They contain requirements and notes for use of the HiCommand Device Manager Agent that may not be fully described in the document. Be sure to review these files, if present, before installing HiCommand Device Manager Agent.

Software Version

This document revision applies to HiCommand® Device Manager version 5.5.

Convention for Storage Capacity Values

Storage capacity values for hard disk drives are calculated based on the following values:

- 1 KB (kilobyte) = 1,000 bytes
- 1 MB (megabyte) = 1,000² bytes
- 1 GB (gigabyte) = 1,000³ bytes
- 1 TB (terabyte) = 1,000⁴ bytes

Storage capacity values for logical devices (LDEVs) on the Universal Storage Platform are calculated based on the following values:

- 1 KB (kilobyte) = 1,024 bytes
- 1 MB (megabyte) = 1,024² bytes
- 1 GB (gigabyte) = 1,024³ bytes
- 1 TB (terabyte) = 1,024⁴ bytes

Referenced Documents

- *HiCommand® Device Manager Web Client Installation and Configuration Guide*, MK-91HC001
- *HiCommand® Device Manager Command Line Interface Application User Guide*, MK-91HC007
- *HiCommand® Device Manager Agent Installation and Configuration Guide*, MK-92HC019
- *TagmaStore™ USP Copy-on-Write Snapshot User's Guide*, MK-95RD277
- *TagmaStore USP and NSC USP Storage Navigator User's Guide*, MK-94RD206

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please see specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
Technical Writing, M/S 35-10
Hitachi Data Systems
10277 Scripps Ranch Blvd.
San Diego, CA 92131

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

Contents

Chapter 1 Introduction to HiCommand® Device Manager

1.1	Overview of HiCommand Device Manager	1
1.2	HiCommand Device Manager Software Components	2
1.3	Basic Configuration.....	2
1.4	Common Component	4
1.5	Related Software Products.....	4
1.5.1	Required Products for the Storage Subsystem	4
1.5.2	Products Related to Device Manager	10
1.6	New Functions in HiCommand Device Manager 5.5	15

Chapter 2 HiCommand Device Manager Network Configuration

2.1	Overview of Network Configuration	17
2.2	Common Security Risks	18
2.3	Server Network Configurations	20
2.3.1	Most Secure Configuration: Separate Management LAN plus Firewall	20
2.3.2	Second-Most Secure Configuration: Separate Management LAN plus Firewalled Devices under Management	21
2.3.3	Third-Most Secure Configuration: Dual-Homed Management Servers plus Separate Management LAN	22
2.3.4	Least Secure Configuration: Flat Network.....	23
2.4	Working With a Network That Uses a Firewall	24
2.5	Registering Firewall Exceptions in a Linux Environment	26
2.5.1	Using the Text Mode Setup Utility	27

Chapter 3 Windows® Systems Installation

3.1	Installation Overview	29
3.1.1	Windows System and Media Requirements	29
3.2	Installing to a Standard Windows Environment	34
3.2.1	Preparing for Installation	34
3.2.2	Performing a New Installation of Device Manager Server.....	39
3.2.3	Performing an Upgrade Installation from Version 3.5 or Earlier	46
3.3	Installing to a Microsoft Cluster Server Environment	59
3.3.1	System Requirements for a Cluster Server	59
3.3.2	Setup Where Other HiCommand Products Are Installed	59
3.3.3	Performing a New Installation.....	62
3.3.4	Performing an Upgrade Installation from Version 3.5 or Earlier	67
3.3.5	Changing to a Cluster Environment after Starting HiCommand Device Manager Server	74
3.4	Converting the Database	76
3.4.1	Manually Converting from InterBase to HiRDB.....	76
3.4.2	Converting to a Cluster Configuration	78
3.5	Verifying Installation of Device Manager Server and Common Component	80
3.5.1	HBase Storage Mgmt Common Service or HBase Storage Mgmt Web Service Fails to Start	81
3.5.2	HBase Storage Mgmt Common or Web Service Does Not Appear in Services.	81

3.5.3	Device Manager Server Fails to Start	81
3.5.4	HiCommand Device Manager Server Does Not Appear in the Services Panel ..	81
3.6	Starting and Stopping Device Manager Server	82
3.6.1	Starting and Stopping Using Windows Functions	82
3.6.2	Starting and Stopping Using Device Manager Commands	82
3.7	Operating the HiCommand Device Manager Server Database	84
3.7.1	Backing Up the Server Database	85
3.7.2	Restoring the Server Database	86
3.7.3	Migrating the Server Database	87
3.7.4	Initializing a HiCommand Device Manager Server Database	93
3.8	Uninstalling the HiCommand Device Manager Server and Related Products.....	94
3.8.1	Uninstalling the HiCommand Device Manager Server in a Standard Environment	94
3.8.2	Uninstalling the Device Manager Server in a Cluster Environment.....	96
3.8.3	Uninstalling InterBase Server and Client	98
3.8.4	Uninstalling InterClient	99

Chapter 4 Solaris and Linux Systems Installation

4.1	Installation Prerequisites for Solaris Systems.....	101
4.1.1	Solaris and Linux System and Media Requirements.....	101
4.2	Managing the LUN and Security Counts.....	104
4.3	Preparing for Installation to a Solaris Environment	106
4.3.1	Preparing for Installation	106
4.3.2	Reviewing the Contents of the Installation CD	110
4.4	Installing Device Manager Server and Common Component.....	111
4.4.1	Upgrading or Re-installing Device Manager	117
4.4.2	Performing an Upgrade Installation from Version 3.5 or Earlier	120
4.4.3	Performing an Upgrade Installation from Version 4.0 or Later or a Re- installation	124
4.5	Installing Device Manager in a Cluster Server Environment	129
4.5.1	System Requirements	129
4.5.2	Setup Where Other HiCommand Products Are Installed	129
4.5.3	Performing a New Device Manager Installation	132
4.5.4	Performing an Upgrade Installation from Version 3.5 or Earlier	144
4.5.5	Performing an Upgrade Installation from Version 4.0 or Later or Performing a Re-installation	149
4.5.6	Converting to a Cluster Configuration	153
4.6	Verifying HiCommand Device Manager Installation.....	155
4.6.1	Verifying the HiCommand Device Manager Server Installation	155
4.6.2	Verifying HiCommand Suite Common Component Installation.....	155
4.7	Starting and Stopping Device Manager Server	156
4.8	Operating the HiCommand Device Manager Server Database	158
4.8.1	Backing Up the Server and Common Component Database	159
4.8.2	Restoring the Server Database.....	160
4.8.3	Migrating the Server Database.....	162
4.8.4	Initializing the Device Manager Server Database	167
4.9	Converting a Device Manager Server Database.....	168
4.9.1	About Converting from InterBase to HiRDB	169
4.9.2	Converting Manually to HiRD8	169
4.10	Uninstalling the HiCommand Device Manager Server and Related Products.....	171

4.10.1	Uninstalling Device Manager Server in a Standard Environment	171
4.10.2	Uninstalling Device Manager Server in a VERITAS Server Environment	173
4.10.3	Uninstalling Device Manager Server in a Sun Cluster Environment	175
4.11	Uninstalling InterBase Components	176
4.11.1	Uninstalling InterBase Server	176
4.11.2	Uninstalling InterClient	177
4.12	Setting Kernel Parameters on Solaris	177
4.12.1	When No Other HiCommand Suite Product (version 4.0 or later) is Installed	177
4.12.2	When Another HiCommand Suite Product (version 4.0 or later) is Installed	180
4.12.3	Setup Needed After Uninstallation of the Device Manager Server	180
4.13	Setting Kernel Parameters and Shell Restrictions on Linux	181
4.13.1	Setup Needed After Uninstallation of the Device Manager Server	183

Chapter 5 Using the HiCommand Suite Common Component

5.1	Installing and Uninstalling HiCommand Suite Common Component	185
5.2	Starting and Stopping HiCommand Suite Common Component	186
5.2.1	Starting the Common Component	186
5.2.2	Stopping the Common Component	187
5.3	Integrated Logging	188
5.3.1	Integrated Log Output	188
5.3.2	Common Component Trace Log Properties	189
5.4	Ports Used By HiCommand Suite Common Component	192
5.4.1	Ports Used by Device Manager Server and Common Component	192
5.4.2	Changing Ports Used by Common Component	193
5.5	Setup for Starting a Web Application from Web Client	197
5.5.1	Using hcmdslink to Register an Application	197
5.5.2	Modifying the URL Information for Starting Web Client	199
5.6	Changing the Host Name of the Management Server	200
5.7	Security Settings for User Accounts	203
5.7.1	password.min.length	204
5.7.2	password.min.uppercase	204
5.7.3	password.min.lowercase	204
5.7.4	password.min.numeric	204
5.7.5	password.min.symbol	204
5.7.6	password.check.userID	204
5.7.7	account.lock.num	205
5.8	Warning Banner Settings	205
5.8.1	Editing the Message	206
5.8.2	Registering the Message	207
5.8.3	Deleting the Message	208

Chapter 6 Setup for Managing Copy Pairs

6.1	Server Requirements for Managing Copy Pairs	209
6.2	Host Requirements for Managing Copy Pairs	209
6.3	Subsystem Requirements for Managing Copy Pairs	211
6.4	Creating Configuration Definition Files	213
6.4.1	Using Device Manager Web Client to Create a Configuration Definition File for CCI	213

Chapter 7 HiCommand Device Manager Server Security

7.1	Overview of HiCommand Device Manager Security	218
7.1.1	About Server and HBase Storage Mgmt Web Service Security	218
7.2	Using HiKeytool to Set Server Security	221
7.2.1	Creating a Keypair	221
7.2.2	Enabling TLS/SSL Server Security	225
7.2.3	Creating and Importing a Digitally-Signed Certificate	227
7.2.4	Displaying Contents of the HiCommand Device Manager Keystore.....	231
7.2.5	Deleting an Entry from HiCommand Device Manager Server Keystore	233
7.2.6	Changing the Device Manager Server Keypass.....	235
7.2.7	Changing the Device Manager Server Keystore Password.....	237
7.2.8	Displaying Contents of HiCommand Device Manager Server Truststore	239
7.2.9	Deleting an Entry from HiCommand Device Manager Server Truststore	241
7.2.10	Changing the HiCommand Device Manager Server Truststore Password	243
7.3	Configuring the HBase Storage Management Web Service for SSL	245
7.3.1	Generating a Private Key Using SSLC	245
7.3.2	Creating a Certificate Signing Request (CSR).....	246
7.3.3	Creating a Self-Signed Certificate.....	248
7.3.4	Configuring SSL	249
7.3.5	About Setting SSL	253
7.4	Security Settings for CIM/WBEM Functionality	255
7.4.1	Modifying the Keystore File for Object Operations.....	255
7.4.2	Specifying Two-Way Authentication for Object Operations.....	258
7.4.3	Procedure for Specifying Two-way Authentication for Event Indications...	261
7.4.4	Procedure for Disabling Two-way Authentication	265
7.5	Authenticating File Operations Using a Java Tool	267
7.5.1	Creating a Keystore File	267
7.5.2	Exporting an Authentication File from a Keystore File	269
7.5.3	Creating a Truststore File and Importing an Authentication File	269

Chapter 8 HiCommand Device Manager Server Properties

8.1	Overview of HiCommand Device Manager Server Properties.....	271
8.2	Server Configuration Properties	276
8.2.1	server.http.host.....	276
8.2.2	server.http.port.....	277
8.2.3	server.https.port.....	277
8.2.4	server.http.default	277
8.2.5	server.http.request.timeout	278
8.2.6	server.http.connection.priority	278
8.2.7	server.http.connection.bufSize.....	278
8.2.8	server.http.socket.backlog.....	278
8.2.9	server.http.socket.maxThreads	279
8.2.10	server.http.socket.linger	279
8.2.11	server.http.socket.noDelay	279
8.2.12	server.http.headers.maxNumber.....	279
8.2.13	server.http.headers.maxLength.....	280
8.2.14	server.http.entity.maxLength	280
8.2.15	server.http.log.reverseDNS.....	280
8.2.16	server.http.cache.size	280

8.2.17	server.http.cache.maxFileSize	281
8.2.18	server.http.fileTypes.noLog	281
8.2.19	server.http.mode	281
8.2.20	server.installTime	281
8.2.21	server.base.home	282
8.2.22	server.horcmconfigfile.hostname	282
8.2.23	server.base.initialsynchro	282
8.2.24	server.cim.support	282
8.2.25	server.cim.support.protocol	283
8.2.26	server.cim.http.port	283
8.2.27	server.cim.https.port	283
8.2.28	server.configchange.enabled	283
8.2.29	server.configchange.autorefresh.lastrefreshed	283
8.3	Database Properties	284
8.3.1	dbm.traceSQL	284
8.3.2	dbm.startingCheck.retryCount	284
8.3.3	dbm.startingCheck.retryPeriod	284
8.4	Logger Properties	285
8.4.1	logger.loglevel	285
8.4.2	logger.MaxBackupIndex	285
8.4.3	logger.MaxFileSize	285
8.4.4	logger.hicommandbase.loglevel	286
8.4.5	logger.hicommandbase.sysloglevel	286
8.4.6	logger.hicommandbase.MaxBackupIndex	286
8.4.7	logger.hicommandbase.MaxFileSize	286
8.5	Dispatcher Properties	287
8.5.1	server.dispatcher.agent.priority	287
8.5.2	server.dispatcher.message.timeout	287
8.5.3	server.dispatcher.message.timeout.in.processing	287
8.5.4	server.dispatcher.daemon.pollingPeriod	288
8.5.5	server.dispatcher.traps.purgePeriod	288
8.5.6	server.dispatcher.startTimeOfIgnoringConnectionAlert	288
8.5.7	server.dispatcher.endTimeOfIgnoringConnectionAlert	288
8.5.8	server.dispatcher.daemon.receiveTrap	288
8.6	MIME Properties	289
8.7	Client Properties	289
8.7.1	client.logger.trace	289
8.7.2	client.message.timeout	290
8.7.3	client.outpuhorcmfunction.enabled	290
8.7.4	table.ldev.rowsperpage	290
8.7.5	client.assignlun.upperlimit.enabled	291
8.8	Security Properties	291
8.8.1	server.http.secure	291
8.8.2	server.http.security.realm	293
8.8.3	server.http.security.clientIP	293
8.8.4	server.https.security.keystore	293
8.8.5	server.https.keystore.passphrase	294
8.8.6	server.https.keystore.keypass	294
8.8.7	server.http.security.unprotected	294
8.8.8	server.https.security.truststore	295

8.8.9	server.https.truststore.passphrase	295
8.9	SNMP Trap Properties	295
8.9.1	Log output customization	296
8.9.2	customizedsnmptrap.customizedSNMPTrapEnable	297
8.9.3	customizedsnmptrap.customizelist	297
8.10	Launchable Applications Properties	298
8.10.1	Launchapp.damp.url	298
8.10.2	launchapp.snm.rmi.port	298
8.11	Mainframe Host Agent Properties	299
8.11.1	host.mf.agent.connection.timeout	299
8.12	Restrictions on Web Clients Connected to the Device Manager Server	299

Chapter 9 Linking Device Manager With Other Products

9.1	Linking With Storage Navigator Modular (for Web)	303
9.1.1	Prerequisites for Using Storage Navigator Modular (for Web)	303
9.1.2	Setting the Launch Environment for Storage Navigator Modular (for Web)	304
9.1.3	Deleting Launch Settings	307
9.1.4	Accessing a Storage Subsystem with Password Protection or Account Authentication Enabled	308
9.2	Linking With DAMP (for Web)	308
9.2.1	Prerequisites for Using DAMP (for Web)	308
9.2.2	Setting the Launch Environment When Using DAMP (for Web)	310
9.2.3	Storage Subsystem Information to be Registered by Using DAMP (for Web)	312
9.3	Starting HSSM From the Dashboard	312

Chapter 10 Troubleshooting

10.1	Problems and Solutions	315
10.2	Collecting Maintenance Information	323
10.2.1	Using hcmdsgetlogs to Acquire Log Files	323
10.2.2	Obtaining a Thread Dump	324
10.3	Contacting the Hitachi Data Systems Support Center	325

Chapter 11 Overview and Setup of CIM/WBEM

11.1	Device Manager and CIM/WBEM)	327
11.2	CIM/WBEM Features of Device Manager	329
11.3	Preparations for Operating the CIM/WBEM Features	330
11.3.1	Basic Settings Required to Use the CIM/WBEM Features	330
11.3.2	Setting up the Ports Used by CIM/WBEM Features	332
11.4	Properties File Settings When Executing CIM	334
11.4.1	The server.properties File	334
11.4.2	The jserver.properties File	335
11.4.3	Saving the cimom.properties File	336
11.5	Setting the Service Discovery Feature	336
11.5.1	Setting Up the Service Discovery Feature	337
11.5.2	Starting and Stopping the Service Discovery Feature	339
11.5.3	Notes on Using OpenSLP	340
11.6	User Permissions for Using CIM/WBEM Features	340

Chapter 12 Overview and Setup of VDS

12.1 About Device Manager VDS Provider	343
12.1.1 Overview of Device Manager VDS Provider	343
12.1.2 Functions of Device Manager VDS Provider	343
12.1.3 Available Functions in Storage Manager for SANs for Windows Server 2003 R2	344
12.2 Installation Requirements and Procedures	345
12.2.1 Installing Device Manager VDS Provider	345
12.2.2 Uninstalling Device Manager VDS Provider	348
12.3 Operating Device Manager VDS Provider	349
12.3.1 Starting and Stopping Device Manager VDS Provider	349
12.3.2 Device Manager VDS Provider Property Files	350
12.3.3 Changing Device Manager VDS Provider Settings	352
12.3.4 Device Manager VDS Provider Log Files	354
Acronyms and Abbreviations	357
Index	359

List of Figures

Figure 1.1	Basic System Configuration of Device Manager	3
Figure 2.1	Incorrect 9900 and 9900V LAN Connection	18
Figure 2.2	Most Secure Configuration: Separate Management LAN Plus Firewall.....	21
Figure 2.3	Second-Most Secure Configuration: Separate Management LAN plus Firewalled Devices.....	22
Figure 2.4	Third-Most Secure Configuration: Dual-Homed Management Servers Plus Separate Management LAN	23
Figure 2.5	Least-Secure Configuration: Flat Network.....	24
Figure 3.1	Choose Install Folder Panel	43
Figure 3.2	Choose the Database for HiCommand Suite Common Component Panel.....	43
Figure 3.3	Choose the Database for HiCommand Device Manager Panel.....	44
Figure 3.4	Installation Server Information Settings.....	44
Figure 3.5	Setting for the SMI-S Provider Service Panel	45
Figure 3.6	Setting for the SMI-S SSL Panel	45
Figure 3.7	Setting for the SLP Service Panel	46
Figure 3.8	Database Conversion Panel.....	52
Figure 3.9	Database Convert Error Panel.....	52
Figure 3.10	Do you want to back up the database? Panel	58
Figure 3.11	Do you want to export the database? Panel	59
Figure 3.12	Warning Panel	96
Figure 3.13	Microsoft Management Console Error Message 997	99
Figure 4.1	Message that Confirms the Setup of the Kernel Parameter	114
Figure 4.2	Error Message for the Setup of the Kernel Parameter	114
Figure 4.3	Message that Confirms Stopping of Services (appears during installation)	114
Figure 4.4	Message Notifying that Another HiCommand Suite Product Is Running (appears during installation)	114
Figure 4.5	Backup Recommendation Reminder	114
Figure 4.6	Available Packages for Installation.....	115
Figure 4.7	SNMP Trap Note	115
Figure 4.8	Settings for the SNMP Trap Reception Function	115
Figure 4.9	Specifying Common Component Database Files.....	115
Figure 4.10	Specifying HiCommand Device Manager Database Files	115
Figure 4.11	Entering IP address and Port Number.....	116
Figure 4.12	Settings for the SMI-S Provider Service.....	116
Figure 4.13	SSL Settings for SMI-S.....	116
Figure 4.14	Changing the Port Number	116
Figure 4.15	Two-way Authentication for Object Operations and Event Indications	116
Figure 4.16	Setting the SLP Daemon	116
Figure 4.17	Installing Device Manager	117
Figure 4.18	Secure Socket Certificates Note	117
Figure 4.19	When InterBase is Not Installed	123
Figure 4.20	Incorrect InterBase Version	123
Figure 4.21	InterClient Not Installed	123
Figure 4.22	Incorrect InterClient Version.....	123
Figure 4.23	Upgrade Error Message.....	123

Figure 4.24	Downgrade Error Message	124
Figure 4.25	Database Conversion Message	124
Figure 4.26	Data Update Error Message	124
Figure 4.27	Database Conversion Confirmation Message	124
Figure 4.28	Selection Message for Backing Up the Database	128
Figure 4.29	Selection Message for Exporting the Database	128
Figure 4.30	Backup Directory Deletion Confirmation Message.....	128
Figure 4.31	Export Directory Deletion Confirmation Message	128
Figure 4.32	Message that Confirms Stopping of Services (appears during uninstallation)..	173
Figure 4.33	Message Notifying that Another HiCommand Suite Product Is Running.....	173
Figure 5.1	Hitachi Network Objectplaza Trace Utility 2 Panel.....	190
Figure 5.2	Displayed Results After Registering the Message	206
Figure 7.1	HiKeytool Main Panel	223
Figure 7.2	Server Main Panel	223
Figure 7.3	Creating a Keypair	224
Figure 7.4	Default Device Manager Server Security Level	226
Figure 7.5	Selecting and Confirming Server Security Level Changes	226
Figure 7.6	Completed CSR	228
Figure 7.7	Sample Certificate Request.....	228
Figure 7.8	Sample Digitally-Signed Certificate	229
Figure 7.9	Entering the Location of the Digitally-Signed Certificate Location (Windows)	230
Figure 7.10	Notification of Successful Import of Digitally-Signed Certificate.....	230
Figure 7.11	Sample Contents of Device Manager Server Keystore	231
Figure 7.12	Sample Verbose Contents of Device Manager Server Keystore.....	232
Figure 7.13	Entering the Number of Alias to be Deleted	234
Figure 7.14	Confirming Deletion of an Alias	234
Figure 7.15	Entering the Current Keystore Password	235
Figure 7.16	Entering the Old Keypass.....	236
Figure 7.17	Entering and Confirming the New Keypass	236
Figure 7.18	Entering Old Keystore Password	237
Figure 7.19	Entering New Keystore Password	238
Figure 7.20	Confirming New Keystore Password	238
Figure 7.21	Contents of Device Manager Server Truststore	239
Figure 7.22	Displaying Verbose Information for Device Manager Truststore	240
Figure 7.23	Entering the Alias to be Deleted from Truststore	242
Figure 7.24	Confirming the Alias to be Deleted From Truststore	242
Figure 7.25	Entering the Current Truststore Password	244
Figure 7.26	Entering and Confirming New Truststore Password.....	244
Figure 7.27	Output of # ./sslc genrsa -out demoCA/httpsdkey.pem 1024 Command	246
Figure 7.28	sslc req Utility Prompts	247
Figure 7.29	Sample Output of a sslc x509 Command.....	248
Figure 7.30	Enabling SSL (Windows)	250
Figure 7.31	Enabling SSL (Solaris or Linux)	251
Figure 7.32	Disabling SSL (Windows).....	251
Figure 7.33	Disabling SSL (Solaris or Linux).....	252
Figure 7.34	Editing Format for the httpsd.conf File	253
Figure 7.35	MOF File Example	256

Figure 8.1	Sample Log Customization (1)	297
Figure 8.2	Format for Registering Hosts in the <code>httpsd.conf</code> File.....	300
Figure 8.3	Example of Registering Hosts to the <code>httpsd.conf</code> File.....	300
Figure 11.1	CIM Components for Device Manager	328

List of Tables

Table 1.1	Prerequisite Firmware Versions and Software Products (for the TagmaStore AMS/WMS series)	4
Table 1.2	Prerequisite Firmware Versions and Software Products (for TagmaStore USP) ..	6
Table 1.3	Prerequisite Firmware Versions and Software Products (for Lightning 9900V) ...	6
Table 1.4	Prerequisite Firmware Versions and Software Products (for Lightning 9900)	7
Table 1.5	Prerequisite Firmware Versions and Software Products (for Thunder 9500V)	8
Table 1.6	Prerequisite Firmware Versions and Software Products (for Thunder 9200).....	9
Table 1.7	Prerequisite Firmware Versions and Software Products (for Sun T3)	10
Table 1.8	Versions of Dynamic Link Manager Supported by Device Manager.....	11
Table 1.9	Versions of Tuning Manager Supported by Device Manager.....	12
Table 1.10	Versions of Provisioning Manager Supported by Device Manager	12
Table 1.11	Versions of Protection Manager Supported by Device Manager	12
Table 1.12	Versions of Tiered Storage Manager Supported by Device Manager	13
Table 1.13	Versions of Replication Monitor Supported by Device Manager	13
Table 1.14	Versions of Global Link Availability Manager Supported by Device Manager ...	13
Table 1.15	Versions of Mainframe Agent Supported by Device Manager	14
Table 2.1	Ports Used for Communication Between the Management Server and a Management Client	24
Table 2.2	Ports Used for Communication Between the Management Server and a Managed Host	25
Table 2.3	Ports Used for Communication Between Management Server and Storage Subsystems	25
Table 2.4	Ports Used for Management Server to CIM Client Communication	26
Table 2.5	Port Used for Communication Between the Management and Mail Servers.....	26
Table 2.6	Port Used for Management Client to Storage Subsystem Communication.....	26
Table 3.1	List of Windows Versions on Which HiCommand Device Manager Server Runs .	30
Table 3.2	Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed	31
Table 3.3	Installation Path and Required Disk Space	31
Table 3.4	Maximum Value of the Number of Resources that Can Be Managed by the HiCommand Device Manager Server	32
Table 3.5	Storage Destination of Backed up and Exported Data and Required Disk Space	56
Table 3.6	Settings to Register HiRDB as a Resource	66
Table 3.7	Settings to Register the HBase Storage Mgmt Common Service as a Resource .	66
Table 3.8	Settings to Register the HBase Storage Mgmt Web Service as a Resource	66
Table 3.9	Settings to Register the HiCommand Device Manager Server as a Resource....	67
Table 3.10	Return Codes for migrateFmIB Command	77
Table 3.11	status2 Return Codes	83
Table 3.12	Backing Up and Restoring Verses Exporting and Importing	84
Table 3.13	Action to Be Taken When an Error Message Is Output (During an Export)	90
Table 3.14	Action to Be Take When an Error Message Is Output (During an Import)	92
Table 4.1	The OSs on Which the HiCommand Device Manager Server Can Run (Solaris) .	101
Table 4.2	The OSs on Which the HiCommand Device Manager Server Can Run (Linux) ..	102
Table 4.3	Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed (Solaris)	102

Table 4.4	Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed (Linux)	102
Table 4.5	Installation Path and Required Disk Space	103
Table 4.6	Maximum Number of Resources Managed by the HiCommand Device Manager Server	104
Table 4.7	Storage Destination of Backed up and Exported Data and Required Disk Space	126
Table 4.8	status2 Return Codes	157
Table 4.9	Backing Up and Restoring Verses Exporting and Importing	158
Table 4.10	Action to Be Taken When an Error Message Is Output (During an Export)	164
Table 4.11	Action to Be Take When an Error Message Is Output (During an Import)	166
Table 4.12	Return codes for the migrateFmIB Command	170
Table 4.13	Recommended values for kernel parameters (for Solaris 8 or Solaris 9)	179
Table 4.14	Recommended values for kernel parameters (for Solaris 10)	179
Table 4.15	Recommended Values for Shell Restrictions (/etc/security/limits.conf)	182
Table 4.16	Recommended Values for Kernel Parameters (/etc/sysctl.conf)	182
Table 5.1	Device Manager Common Component Elements	186
Table 5.2	Integrated Log Output	189
Table 5.3	Device Manager Server and Common Component Ports	192
Table 5.4	Example of Editing a Message	206
Table 6.1	Copy Pair Operations and Required Versions of Device Manager Agent	209
Table 6.2	Subsystem Requirements	211
Table 8.1	Summary of Device Manager Property Files	273
Table 8.2	Format of Each Item Used for Customization Definition	297
Table 9.1	launchapptool Input Example (When Setting Storage Navigator Modular (for Web))	306
Table 10.1	General Troubleshooting Information	315
Table 11.1	Correspondence Between Namespaces and SMI-S Versions	328
Table 11.2	Port Number Used by CIM/WBEM Features	331
Table 11.3	Setting Values for server.cim.support.protocol	332
Table 11.4	Properties You Must Set for Device Manager Server When Executing CIM	334
Table 11.5	User Permissions for Using CIM/WBEM Features	341
Table 12.1	logger.properties File	351
Table 12.2	hdvconfig Command Syntax and Functions	354
Table 12.3	Log Files	354

Chapter 1 Introduction to HiCommand® Device Manager

This chapter discusses the following topics:

- Overview of HiCommand Device Manager (see section 1.1)
- HiCommand Device Manager Software Components (see section 1.2)
- Basic Configuration (see section 1.3)
- Common Component (see section 1.4)
- Related Software Products (see section 1.5)
- New Functions in HiCommand Device Manager 5.5 (see section 1.6)

1.1 Overview of HiCommand Device Manager

HiCommand Device Manager provides a consistent, easy to use, and easy to configure interface for managing storage products. Device Manager provides a web-based graphical client interface for real-time interaction with managed storage arrays, as well as a command line interface (CLI) for scripting. Device Manager gives storage administrators access to the configuration, monitoring, and management features that are already integrated into existing Hitachi Data Systems software products.

Device Manager allows you to view the configuration of the storage subsystems added to the Device Manager system, and perform configuration operations such as allocating storage or securing LUNs. You can quickly discover storage subsystems based on key attributes, and efficiently manage complex and heterogeneous storage environments, even remotely through SSL-based communications. Device Manager also enables you to back up and restore your configuration database.

More specifically, HiCommand Device Manager provides:

- Storage subsystem discovery and configuration display
- Hierarchical group management for storage
- Alert presentation
- Volume (LUN) configuration
- Management of hosts and WWNs.
- Remote access to Disk Array Management Program (DAMP)

Device Manager also provides several levels of access and functionality for end users, including Access Control, Storage Management and System Support:

- Access Control handles support for the system administrator, storage administrator, maintenance user and guest user
- Storage Management handles storage configuration and manipulation

- System Support handles user administration, monitoring host agent activity and management of LUN security

Caution: When you change storage subsystem configuration information using HiCommand Device Manager, we recommend that you back up the information beforehand. For details on how to back up such information, see the manual for the relevant subsystem.

Important: HiCommand Device Manager cannot be used to set information for mainframe volumes, however, it can be used to reference such volume information when that information is handled by TagmaStore USP, Lightning 9900V, or Lightning 9900.

1.2 HiCommand Device Manager Software Components

This document describes and provides instructions for installing and configuring the Device Manager Server. HiCommand Device Manager consists of the following basic components:

Server. Device Manager Server communicates with Hitachi Data Systems 9900 V Series, 9900, 9500 V Series, 9200, and Sun T3 storage subsystems. In addition, the Device Manager Server manages client connections with the Device Manager Web Client and the Device Manager Host Agent(s) using the http protocol. The Device Manager Agent and the Device Manager Server can be installed on the same host machine.

Web Client. Device Manager Web Client is a web-based user interface for Device Manager functionality. The Web Client is a stand-alone Java-based application that is deployed using the Java Web Start (JWS) software. It communicates with and runs as a client of the Device Manager Server. For further information on Device Manager Web Client, see the *HiCommand Device Manager Web Client User's Guide*.

Command Line Interface (CLI). Device Manager CLI enables you to perform client operations by issuing commands from the system command-line prompt. For further information on the command-line interface, see the *HiCommand Device Manager Command Line Interface Application User Guide*.

Host Agent. Device Manager agent on a host runs on host computers attached to storage subsystems managed by Device Manager. The Host Agent collects data on the configuration and utilization of the attached storage and sends this information to the Device Manager Server. For further information on the Device Manager Host Agent, see the *HiCommand Device Manager Agent Installation Guide*. The Device Manager Agent and the Device Manager Server can be installed on the same host machine.

Device Manager VDS Provider. The Device Manager VDS provider is software that allows you to provide storage subsystem information in response to requests from VDS (Virtual Disk Service), a virtual disk service provided by Windows Server 2003, and to change storage subsystem configuration.

1.3 Basic Configuration

Figure 1.1 shows a basic Device Manager system configured for storage subsystem configuration management.

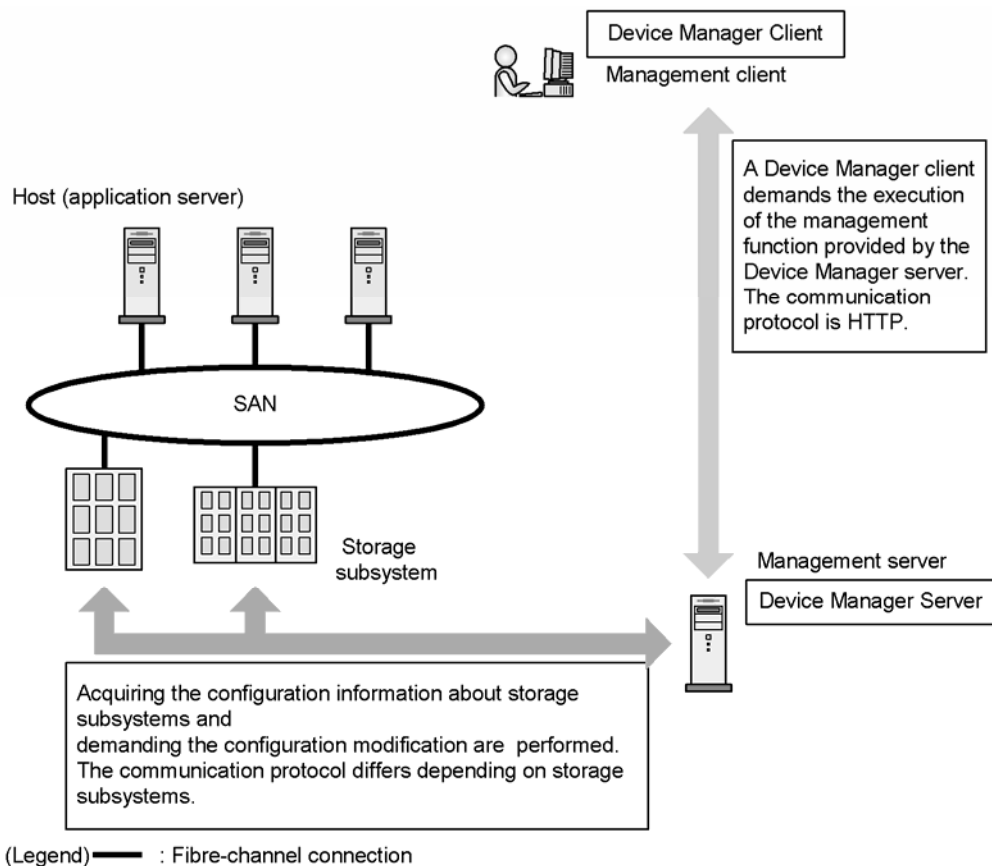


Figure 1.1 Basic System Configuration of Device Manager

When you need only to manage the configuration of storage subsystems, and do not need to manage the storage usage statuses from a host, you can construct the type of system illustrated in Figure 1.1

Note the following about Figure 1.1:

- The *management client* refers to the machine on which a Device Manager client runs.
- The *management server* refers to the machine on which the Device Manager server runs.
- A management client and a management server can be the same machine.
- The *host* refers to the machine that uses the volumes provided by a storage subsystem.
- A TCP/IP network must connect the management client and the management server.
- The HTTP protocol is used for communications.
- A TCP/IP network must connect the management server and the storage subsystem.
- The communication protocol used between a management server and a storage subsystem varies from one storage subsystem to another.
- A management server and a management client need not be connected to a storage subsystem by a Fibre Channel connection.

1.4 Common Component

HiCommand Suite Common Component is a package of features that are used by all HiCommand Suite products. It is installed as part of the Device Manager installation. The Common Component is discussed in detail in Chapter 5. Each HiCommand Suite product bundles the Common Component to use the following functions:

- HBase Storage Mgmt Common Service
- Integrated logging and repository
- HBase Storage Mgmt Web Service

1.5 Related Software Products

1.5.1 Required Products for the Storage Subsystem

When managing storage subsystems, you use management tools and application program interfaces (APIs) other than the HiCommand Device Manager components.

Caution: When you replace the microcode for a storage subsystem that is already registered as a Device Manager management target, you do not need to stop the HiCommand Device Manager server. Note, however, that the configuration of the storage subsystem must not be changed at this time (by performing, for example, refresh and path operations). After the microcode has been successfully replaced, refresh the storage subsystem.

Caution: When Physical View of the TagmaStore Universal Storage Platform(USP) or Storage Navigator of the Lightning 9900V is launched, Java Web Start and the Web browser on the Web Client machine directly communicate with the storage subsystem. For this reason, if the Web Client machine and the storage subsystem exist on different networks, you must set up the networks so that the machine and the storage subsystem can directly communicate with each other.

This section describes the storage subsystem requirements for using Device Manager.

1.5.1.1 Required for the TagmaStore AMS/WMS Series

The Linux version does not support the TagmaStore AMS/WMS series.

The following table describes the prerequisite firmware versions and software products:

Table 1.1 Prerequisite Firmware Versions and Software Products (for the TagmaStore AMS/WMS series)

Prerequisite firmware versions	Prerequisite software products
■ TagmaStore AMS microcode: Any	To set up security for LUNs: ■ LUN Manager^{#1}
■ TagmaStore WMS microcode:	To use LUSE:

Prerequisite firmware versions	Prerequisite software products
Any	▪ LUN Expansion To use a lock system for devices accessed from HiCommand Device Manager: ▪ Password Protection ▪ Account Authentication To use the copy pair functionality: ▪ ShadowImage in-system replication ▪ TrueCopy remote replication^{#2} ▪ TrueCopy Extended Distance ▪ COW Snapshot To use Physical View: ▪ Storage Navigator Modular (for Web)

#1 If you want to use HiCommand Device Manager to configure LUN security, you need to use Storage Navigator Modular (for Web) or DAMP (for Web) to enable the mapping mode of LUN Manager. Make sure that the mapping mode of the storage subsystem is *M-TID*, *M-LUN*. When the mapping mode is disabled, you cannot use LUN Manager.

#2 For details on the models that support TrueCopy, see the *TrueCopy Remote Replication User's Guide*.

Caution: The Device Manager server communicates over TCP/IP to manage the TagmaStore AMS/WMS series and Thunder 9500V series storage subsystems. If you want to change the default port number (2000) used by all these storage subsystems for TCP/IP communication, you must set the new port number in the `services` file for the machine where the Device Manager server has been installed. If you operate the storage subsystems without setting the new port number in the `services` file, an error (code:DMEA000006) might occur and the operation might fail. If the port number of some storage subsystems is set to the default (2000) and the port number of other storage subsystems is set to a new number, and the new port number is specified in the `services` file, an error does not occur (although the operation might take a long time). For details on how to check the port number and how to set the `services` file, see the manual for the TagmaStore AMS/WMS series and Thunder 9500V series.

Note: For a NAS Modular subsystem of the TagmaStore AMS/WMS series, HiCommand Device Manager only allows you to add storage subsystems and to launch Storage Navigator Modular. To operate a NAS Modular subsystem, perform the operations from Storage Navigator Modular.

1.5.1.2 Required for TagmaStore USP

The following table describes the prerequisite firmware versions and software products:

Table 1.2 Prerequisite Firmware Versions and Software Products (for TagmaStore USP)

Prerequisite firmware versions	Prerequisite software products
- Controller microcode: 50-00-00-xx/xx or later - Controller microcode to use CLIEX functions: 50-03-95-xx/xx or later	- JAVA API - SNMP API - LUN Manager To use functions for creating a LUSE or LDEV (CVS): - OPEN Volume Management To use the copy pair functionality: - ShadowImage - TrueCopy - TrueCopy Asynchronous - Universal Replicator - COW Snapshot[#] To use Physical View: - Storage Navigator To link with NAS Manager: - NAS Blade Manager To use Universal Volume Manager: - Universal Volume Manager To use storage logical partitioning (SLPR) or cache logical partitioning (CLPR): - Virtual Partition Manager

[#] For details on the models that support COW Snapshot, see the *Copy-on-Write Snapshot User's Guide*.

1.5.1.3 Required for Lightning 9900V

The following table describes the prerequisite firmware versions and software products:

Table 1.3 Prerequisite Firmware Versions and Software Products (for Lightning 9900V)

Prerequisite firmware versions	Prerequisite software products
- Controller microcode: 21-01-25-xx/xx or later - Controller microcode to perform in-context launching of the Storage Navigator: 21-04-04-xx/xx or later	- Java API - SNMP API - LUN Management To use functions for creating a LUSE or LDEV (CVS): - Open Volume Management

Prerequisite firmware versions	Prerequisite software products
▪ Controller microcode to launch NAS Manager: 21-04-00-xx/xx or later ▪ Controller microcode to use CLIEX functions: 21-14-02-xx/xx or later	To use the copy pair functionality: ▪ Hitachi ShadowImage ▪ Hitachi TrueCopy To link with Storage Navigator: ▪ Storage Navigator To link with NAS Manager: ▪ NAS/Management

For more information on installing and configuring program products, see the *9900V Remote Console – Storage Navigator User's Guide*.

1.5.1.4 Required for Lightning 9900

The following table describes the prerequisite firmware versions and software products:

Table 1.4 Prerequisite Firmware Versions and Software Products (for Lightning 9900)

Prerequisite firmware versions	Prerequisite software products
▪ Controller microcode: 01-18-09-00/00 or later ▪ Controller microcode to use CLIEX functions: 01-19-59-xx/xx or later	▪ SNMP Agent ▪ LUN Manager (LUNM) To set up security for LUNs: ▪ LUN Security To use functions for creating a LUSE or LDEV (CVS): ▪ LU Size Expansion (LUSE) ▪ Open Customizable Volume Size (OCVS) To use the copy pair functionality: ▪ Hitachi Multi-RAID Coupling Feature ▪ Hitachi Remote Copy ▪ Hitachi Remote Copy Asynchronous

Requirements not related to firmware versions or software products are as follows:

If you are setting up an alias for HPAV (Hitachi Parallel Access Volume), the LDEV number assigned for both the base volume and the alias volume must be in the same 32-LDEV boundary (for example, 0 to 31, 32 to 63). If they are not the same, you may get the following error message when you try to create an LDEV:

The volume to be created by the CVS operation is being used as the MAV function.

- For more information on PAV, see *Hitachi Lightning 9900 Parallel Access Volume User's Guide*.
- For more information on installing and configuring program products, see *Hitachi Lightning 9900 Remote Console User's Guide*.

1.5.1.5 Required for Thunder 9500V

Caution: The Linux version does not support Thunder 9500V.

The following table describes the prerequisite firmware versions and software products:

Table 1.5 Prerequisite Firmware Versions and Software Products (for Thunder 9500V)

Prerequisite firmware versions	Prerequisite software products
▪ Thunder 9570V or Thunder 9530V microcode: 0651 or later ▪ Thunder 9580V microcode: 1655/B or later ▪ Thunder 9585V microcode: 1657/A or later ▪ Microcode required to use QuickShadow: 0655/D or later^{#1}, 1655/D or later^{#2} ▪ Microcode required to use SATA expansion enclosure: 0658 or later^{#1}, 1658 or later^{#2}	To set up security for LUNs: ▪ Fibre security control functionality or LUN Management^{#3} To use LUSE: ▪ LUN Expansion To use a lock system for devices accessed from HiCommand Device Manager: ▪ Password Protection To use the copy pair functionality: ▪ Hitachi ShadowImage ▪ Hitachi TrueCopy Basic ▪ Hitachi QuickShadow

#1: For Thunder 9570V or Thunder 9530V

#2: For Thunder 9580V or Thunder 9585V

#3 If you want to use HiCommand Device Manager to configure LUN security, you need to use Storage Navigator Modular (for Web) or DAMP (for Web) to enable the mapping mode of LUN Manager. When the mapping mode is disabled, you cannot use LUN Manager.

Requirements not related to firmware versions or software products are as follows:

- Before installation, use DAMP (for Web) or Storage Navigator Modular (for Web) to verify that there are no ports with a WWN node name consisting only of zeros. If there are, you must change the name or delete the WWN, or a node-name error message will be output.

- If the Password Protection option is installed and usable, any addition of a storage subsystem to HiCommand Device Manager requires a Password Protection user ID and password.

Caution: The Device Manager server communicates over TCP/IP to manage the TagmaStore AMS/WMS series and Thunder 9500V series storage subsystems. To change the default port number (2000) used by all these storage subsystems for TCP/IP communication, you must set the new port number in the `services` file for the machine where the Device Manager server has been installed. If you operate the storage subsystems without setting the new port number in the `services` file, an error (code:DMEA000006) might occur and the operation might fail. If the port number of some storage subsystems is set to the default (2000) and the port number of other storage subsystems is set to a new number, and the new port number is specified in the `services` file, an error does not occur (although the operation might take a long time). For details on how to check the port number and how to set the `services` file, see the manual for the TagmaStore AMS/WMS series and Thunder 9500V series.

1.5.1.6 Required for Thunder 9200

Caution: The Linux version does not support Thunder 9200.

Note: SCSI models are not supported.

The following table describes the prerequisite firmware versions and software products:

Table 1.6 Prerequisite Firmware Versions and Software Products (for Thunder 9200)

Prerequisite firmware versions	Prerequisite software products
Microcode: 0559 or later, 355E or later	To set up security for LUNs: ▪ Fibre security control functionality To use LUSE: ▪ LU integration functionality To use a lock system for devices accessed from HiCommand Device Manager: ▪ Password Protection To use the copy pair functionality: ▪ MRCF-Lite Remote Pack ▪ Synchronous Remote Copy function

Requirements not related to firmware versions or software products are as follows:

- Make sure that fibre-channel ports are supported, because HiCommand Device Manager does not support SCSI models.

- Make sure that the mapping mode of the storage subsystem is M-TID, M-LUN. If you attempt to perform an LUN management operation from HiCommand Device Manager when the mapping mode is not M-TID, M-LUN, an error may occur.

Important: Do not use Dynamic Host Configuration Protocol (DHCP) when you use Device Manager to manage the storage subsystem. Use DAMP (for Web) or Storage Navigator Modular (for Web) to make sure that DHCP is not selected.

Note: The Thunder 9200 series supports functionality to reserve LUNs for volumes that are not defined on it. If a user tries to assign such a reserved LUN to the storage unit for an applicable port, Device Manager displays an error message.

1.5.1.7 Required for Sun T3 Only

Note: Device Manager can use the T3 in either a stand-alone configuration (single tray) or a partner pair configuration:

The following table describes the prerequisite firmware versions and software products:

Table 1.7 Prerequisite Firmware Versions and Software Products (for Sun T3)

Prerequisite firmware versions	Prerequisite software products
Firmware: 1.1.7, 1.1.8, 2.0.0, or 2.0.1	None

Requirements not related to firmware versions or software products are as follows:

- Perform the initial installation for the T3 according to the procedures described in the Sun Microsystems Corporation documentation, using a telnet interface specific to T3.
- Write down the root password. Managing T3 disk arrays using Device Manager requires the root password (the password that was entered when the disk array was added).

For T3 in the partner pair configuration, when one LDEV has paths through two ports, to display the information acquired by Device Manager Agent on Web Client, you need to use the host bus adapters that meet the following requirements:

- The HBA API must be provided.
- The subsystemPortWWN must be obtainable from **HBA_GetFcpTargetMapping**.

1.5.2 Products Related to Device Manager

Dynamic Link Manager manages the storage access paths to and from the host on which it is installed. The Dynamic Link Manager GUI(Graphical User Interface) can be displayed from the Device Manager Web Client. For more information on Dynamic Link Manager, please see the following documents.

When Dynamic Link Manager 5.8 or later is installed on the host:

- *HiCommand Dynamic Link Manager User's Guide (for AIX)*

- *HiCommand Dynamic Link Manager User's Guide (for Solaris)*
- *HiCommand Dynamic Link Manager User's Guide (for HP-UX)*
- *HiCommand Dynamic Link Manager User's Guide (for Linux)*
- *HiCommand Dynamic Link Manager User's Guide (for Windows)*

When the version of Dynamic Link Manager installed on the host is earlier than 5.8:

- *Hitachi Dynamic Link Manager User's Guide for AIX Subsystems.*
- *Hitachi Dynamic Link Manager User's Guide for HP-UX Subsystems.*
- *Hitachi Dynamic Link Manager User's Guide for Linux Subsystems.*
- *Hitachi Dynamic Link Manager User's Guide for Sun Solaris Subsystems.*
- *Hitachi Dynamic Link Manager User's Guide for Windows NT and Windows 2000 Subsystems.*

Note: The following table describes the versions of Dynamic Link Manager supported by Device Manager.

Table 1.8 Versions of Dynamic Link Manager Supported by Device Manager

Host machine platform	Dynamic Link Manager version
Windows	4.0 or later
Solaris	3.0, 3.0.2, 4.0 or later
AIX	4.0 or later
HP-UX	4.0 or later
Linux	4.0 or later

HiCommand Tuning Manager manages storage performance and capacity, and is installed on a host. You can install Tuning Manager and Device Manager in different hosts. The Tuning Manager GUI can be displayed from Device Manager Web Client.

WARNING: Do not install Tuning Manager version 4.0 or higher on the same server as Device Manager version 4.0 or higher.

For more information on Tuning Manager please see the following documents:

- *HiCommand Tuning Manager Administration Guide.*
- *HiCommand Tuning Manager Reference Guide.*
- *HiCommand Tuning Manager User's Guide.*
- *HiCommand Tuning Manager Installation Guide.*
- *HiCommand Tuning Manager Performance Reporter User's Guide.*

Note: The following table describes the versions of Tuning Manager supported by Device Manager.

Table 1.9 Versions of Tuning Manager Supported by Device Manager

Platform	Tuning Manager version
Windows	1.0.1 or later
Solaris	1.0.1 or later

Provisioning Manager is a product whose purpose is to assign volumes to the server, and to expand file systems easily. Assigning volumes or expanding file systems requires a series of operations such as selecting the most appropriate storage for use, creating device files on the server, and creating and mounting file systems. Provisioning Manager automates such operations, reducing the workload on system administrators. For more information about Provisioning Manager, see the Provisioning Manager documentation:

- *HiCommand Provisioning Manager Installation and Configuration Guide*
- *HiCommand Provisioning Manager User's Guide.*

Note: The following table describes the versions of Provisioning Manager supported by Device Manager.

Table 1.10 Versions of Provisioning Manager Supported by Device Manager

Platform	Provisioning Manager version
Windows	3.5.0 or later
Solaris	3.5.0 or later
Linux	5.1.0 or later

Protection Manager systematically controls storage subsystems, backup-management products, database products, and application products. If you are using Protection Manager, you will need Windows version 3.5 or later. For more information about HiCommand Protection Manager, please see the following documents:

- *HiCommand Protection Manager Command Line Interface User's Guide.*
- *HiCommand Protection Manager Command Reference User's Guide.*
- *HiCommand Protection Manager Error Codes.*
- *HiCommand Protection Manager Console User's Guide.*

Note: The following table describes the versions of Protection Manager supported by Device Manager.

Table 1.11 Versions of Protection Manager Supported by Device Manager

Platform	Protection Manager version
Windows	3.5 or later

Tiered Storage Manager provides a method of transferring data to an appropriate storage subsystem according to the data characteristics (severity level and access frequency). Tiered Storage Manager optimizes the arrangement of data in an environment where multiple storage subsystems are centralized using TagmaStore USP. For more information about Tiered Storage Manager, see the Tiered Storage Manager documentation.

Note: The following table describes the versions of Tiered Storage Manager supported by Device Manager.

Table 1.12 Versions of Tiered Storage Manager Supported by Device Manager

Platform	Tiered Storage Manager version
Windows	4.0.0-01 or later
Solaris	4.3.0 or later

Replication Monitor displays the copy pair configuration for the entire system in a way that is easy to understand from the viewpoint of the configuration definition of hosts, storage subsystems, and copy pairs. You can also set up monitoring so that Replication Monitor automatically notifies the user when an error is detected. For more information about Replication Monitor, see the Replication Monitor documentation.

Note: The following table describes the versions of Replication Monitor supported by Device Manager.

Table 1.13 Versions of Replication Monitor Supported by Device Manager

Platform	Replication Monitor version
Windows	4.0 or later
Solaris	4.0 or later

Global Link Availability Manager provides centralized management of all paths when Dynamic Link Manager is installed on multiple hosts. This can reduce the administrator's workload in a large-scale system because path management does not have to be performed separately for each host. The Global Link Availability Manager GUI can be displayed from Device Manager Web Client. For details on Global Link Availability Manager, see the Global Link Availability Manager documentation.

Note: The following table describes the versions of Global Link Availability Manager supported by Device Manager.

Table 1.14 Versions of Global Link Availability Manager Supported by Device Manager

Platform	Global Link Availability Manager version
Windows	5.0 or later
Solaris	5.0 or later

Mainframe Agent provides volume information on the storage subsystems managed by a mainframe host. This allows subsystems that could only be monitored on the mainframe host system to be monitored from a Device Manager client program, thereby facilitating centralized management of distributed resources. For details on Mainframe Agent, see the Mainframe Agent documentation. For information on setting the environment to link with Mainframe Agent, see the *HiCommand Device Manager Command Line Interface (CLI) User's Guide*.

Table 1.15 Versions of Mainframe Agent Supported by Device Manager

Mainframe host platform	Mainframe Agent version
OS/390 (version: 2.10)	5.1 or later
z/OS (version: 1.4, 1.5, 1.6, or 1.7)	5.1 or later

Command Control Interface (CCI) is installed on a host, and manages TagmaStore, AMS, 9900V, 9900, 9500V and 9200 series from the command line. CCI tasks include collecting information about storage pair configurations and reporting the information to the Device Manager server. For more information about CCI, please see the following documents:

- *Hitachi TagmaStore USP and NSC, Lightning 9900 V Series and 9900 Command Control Interface (CCI) User's Guide.*
- *Hitachi TagmaStore Adaptable Modular Storage-Storage Navigator Modular Command Line Interface (CLI) User's Guide.*
- *Hitachi Thunder 9500 V Series Command Control Interface (CCI) User and Reference Guide.*
- *Hitachi Thunder 9200 Command Control Interface (CCI) User and Reference Guide.*

TrueCopy can create a replica of one or more volumes in a remote subsystem. For more information on TrueCopy please see the following documents:

- *Hitachi TagmaStore USP and NSC TrueCopy User and Reference Guide*
- *Hitachi Lightning 9900 V Series TrueCopy User and Reference Guide*
- *Hitachi Lightning 9900 TrueCopy User and Reference Guide.*
- *Hitachi Thunder 9500 V Series TrueCopy User's Guide.*
- *Hitachi Thunder 9200 TrueCopy User's Guide.*
- *Hitachi TagmaStore Adaptable Modular Storage TrueCopy Synchronous Remote Replication Software User's Guide.*

Universal Replicator, which was developed from a TrueCopy function, can create a replica of volumes in another storage subsystem. For more information about Universal Replicator, please see *Hitachi TagmaStore USP and NSC Universal Replicator User's Guide*.

Hitachi Virtual Partition Manager allows you to partition the storage and the cache of a TagmaStore subsystem.

Note: If you use Device Manager to directly manage storage logical partitions, you will need a separate Device Manager server for each partition. If you use Device Manager to link and launch Storage Navigator, you can use a single server to manage a partitioned subsystem.

For more information about VPM, please see the following documents:

- *Hitachi TagmaStore USP and NSC Virtual Partition Manager User's Guide.*
- *Hitachi TagmaStore Adaptable Modular Storage Cache Partition Manager User's Guide.*
- **ShadowImage** can create a replica of one or more volumes in the same subsystem. For more information on ShadowImage please see the following documents:
 - *Hitachi TagmaStore USP and NSC ShadowImage User's Guide.*
 - *Hitachi TagmaStore Adaptable Modular Storage ShadowImage In-System Replication Software User's Guide.*
 - *Hitachi Lightning 9900 V Series ShadowImage User's Guide.*
 - *Hitachi Lightning 9900 ShadowImage User's Guide.*
 - *Hitachi Thunder 9500 V Series ShadowImage User's Guide.*
 - *Hitachi Thunder 9200 ShadowImage User's Guide.*

Hitachi Copy on Write Snapshot (COW) allows you to internally retain a logical duplicate of the primary volume data, which is used to restore data if a logical error occurs in the primary volume. For more information on Copy on Write Snapshot, see the following documents:

- *Hitachi TagmaStore Adaptable Modular Storage Copy-on-Write Snapshot Software User's Guide.*
- *Hitachi Freedom Storage Thunder 9500 V Series Copy-on-Write Snapshot Software User's Guide.*

HiCommand Storage Services Manager acts as the main console for heterogeneous storage infrastructure management software, providing SAN visualization and reporting, asset management, performance and capacity monitoring and planning, and policy-driven event management.

WARNING: Do not install HSSM on the same server as Device Manager.

For more information about Hitachi Storage Services Manager, please see the following documents:

- *HiCommand Storage Services Manager Installation and Configuration Guide.*
- *User Guide for HiCommand Storage Services Manager, HiCommand Path Provisioning, and HiCommand Chargeback.*
- *HiCommand Storage Services Manager CLI Guide.*

1.6 New Functions in HiCommand Device Manager 5.5

HiCommand Device Manager 5.5 provides the following new function:

- In Device Manager Web Client, the user can now set password conditions, automatic account locking, and warning banner messages as security options.

- In Device Manager Web Client, the user can now switch whether the area, which contains the **Explorer** menu and **Dashboard** menu, is shown or hidden.
- In Device Manager Web Client, **Host**, **EMU Type**, and **External Subsystem** displayed in a sortable table have been added to the objects for the filter function.
- In Device Manager Web Client, the method for selecting a parent group when creating a logical group has been changed.
- Device Manager Web Client now displays only the WWNs of previously selected hosts when adding storage from host management.
- In Device Manager Web Client, the display order of the items in a sortable table has been changed.
- Device Manager server now enables you to select the number of lines that the sortable table can display per page.
- Device Manager server now enables you to make the upper limit check enabled or disabled for the number of LUNs that are assigned when storage is added.
- The database migration function has been added to support machine replacement in connection with the upgrade of HiCommand Suite products.
- Device Manager server now supports installation using remote desktop for Windows Server 2003 x64 Edition, Windows Server 2003 R2, Windows Server 2003 R2 x64 Edition, and Windows XP SP2 (only for console session connection).
- Commands and procedures used for setting up Device Manager server in a cluster environment have been changed.
- Methods for specifying a namespace when the CIM/WBEM features are used have been added.
- Device Manager server now enables you to set the open or close status of dedicated ports used by CIM/WBEM.

HiCommand Device Manager 5.5 provides the following extensions:

- Support for new OSs
 - Device Manager server, Device Manager Web Client, and Device Manager CLI now support Sun Microsystems Solaris 10 (SPARC version).
 - Device Manager server now supports Windows Server 2003 R2
 - Device Manager Web Client and Device Manager CLI now support Windows Server 2003 R2 (x86 processor version).
- Device Manager Web Client HTML GUI and Device Manager CLI now support JRE version 5.0.
- In Device Manager Web Client, the user can now use a maximum of 256 bytes when setting a user ID or password.

Chapter 2 HiCommand Device Manager Network Configuration

This chapter describes network configuration as it relates to security, as follows:

- Overview of Network Configuration (see section 2.1)
- Common Security Risks (see section 2.2)
- Server Network Configurations (see section 2.3)
- Working With a Network That Uses a Firewall (see section 2.4)
- Registering Firewall Exceptions in a Linux Environment (see section 2.5)

2.1 Overview of Network Configuration

TagmaStore USP, Lightning 9900V, and Lightning 9900 come equipped with a service processor, which is known as the SVP. The SVP has two Ethernet adapters. The first adapter is for a private (internal) Ethernet LAN, which is intended for intra-array communications only. There are only two devices that can access the internal LAN: the Service Processor (SVP), and the Remote Console for Lightning 9900. The second adapter is used for other applications to talk to the SVP. This LAN is referred to as the public LAN, because it is visible to other computers outside the array. HiCommand Device Manager, Enterprise Resource Manager and Enterprise Storage Resource Manager applications use the public LAN to communicate with the SVP about the array and configuration changes.

While TagmaStore USP, Lightning 9900V, and Lightning 9900 are managed through their SVP interface, other manageable storage arrays (for example, the TagmaStore AMS/WMS series, 9500V and 9200 arrays and Sun T3 arrays) do not have a private LAN. Instead, these arrays have Ethernet network interfaces that are intended to be directly attached to a public LAN. Once attached to the LAN, each has its own remote management API, which can be accessed by a variety of management applications.

WARNING: TagmaStore USP, Lightning 9900V, and Lightning 9900 have a public LAN and a private LAN. Device Manager uses the public LAN to communicate with the SVP about the array and configuration changes. Do not under any circumstances attach the private LAN to an external network because this can cause serious problems on the array.

Figure 2.1 illustrates an **incorrect** LAN connection.

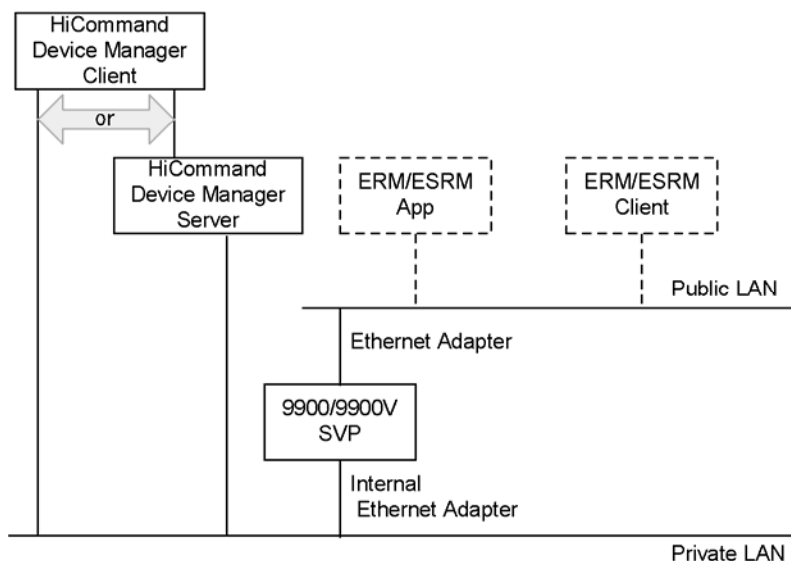


Figure 2.1 Incorrect 9900 and 9900V LAN Connection

For more information on Device Manager requirements for the 9900 V Series, 9900, 9500V, 9200, and T3, please see *HiCommand Device Manager Web Client Installation and Configuration Guide*.

2.2 Common Security Risks

Because the TagmaStore AMS/WMS series, Hitachi Thunder and Sun T3 arrays are intended to be connected to a public LAN, you must pay particular attention to security risks if you are attaching any of these arrays to a public network.

System administrators frequently separate production LANs from management LANs. In such cases, management LANs act as a separate network, which isolates management traffic from a production network and reduces the risk of security-related threats. If a management controller such as the SVP exists on a production LAN, the storage subsystems are left open for any entity on the IP network to access. Whether the access is intentional or not, the resulting security risks can lead to actual outages characterized as Denial of Storage Service (DoS) attacks that may lead to a management session being hijacked for malignant purposes, such as unbinding a storage extent from a port during an I/O operation.

The following are guidelines for constructing management LANs:

- Traffic from the production LAN should not flow through, or be routed to the management LAN.
- If possible, all hosts with management interfaces or controllers on the management LAN should be hardened to their maximum level to reduce the potential that software other than the management interface will not lead to an exploit of the entire station or device. (In this case hardening should include removal of unnecessary software, shutting down nonessential services, and updating to the latest patches.)

- The management LAN should only intersect a production LAN on those hosts acting as an interface between the management LAN and the production LAN (for example, the HiCommand Device Manager Server).
- If possible, those hosts intersecting both private LAN and management LAN should be behind a firewall of some kind, further inhibiting unintended access.

2.3 Server Network Configurations

2.3.1 Most Secure Configuration: Separate Management LAN plus Firewall

In this case, the server hosting Device Manager must either be dual homed or have two NICs, and every other management application must be of similar configuration. The first NIC for each host is attached to a LAN dedicated to management traffic between the management host and devices under management, which for Device Manager includes any TagmaStore AMS/WMS series, TagmaStore USP, 9900s, 9900Vs, 9200, and T3. A second NIC is attached to a LAN where access is governed by a firewall. As shown in Figure 2.2, each server could also be connected to a different LAN with a different firewall. The firewall contains strict access rules that allow access to the management servers only to Device Manager or specified management application clients.

This configuration is the most secure but least flexible implementation, as it requires overhead to manage all of the various network components, servers, and devices under management. Adding further security to this configuration requires that the underlying management application OS be hardened to the maximum possible limit. This might include disabling services such as Telnet, FTP, SMTP, or IIS. Additionally, all unnecessary packages should be removed if possible.

For a comprehensive overview of what is required to harden a server, see <http://ist.uwaterloo.ca/security/howto/>.

Caution: When Physical View of the TagmaStore USP or Storage Navigator of the Lightning 9900V is launched, Java Web Start and the Web browser on the Web Client machine directly communicate with the storage subsystem. For this reason, if the Web Client machine and the storage subsystem exist on different networks, you must set up the networks so that the machine and the storage subsystem can directly communicate with each other.

Figure 2.2 illustrates a separate management LAN plus a firewall.

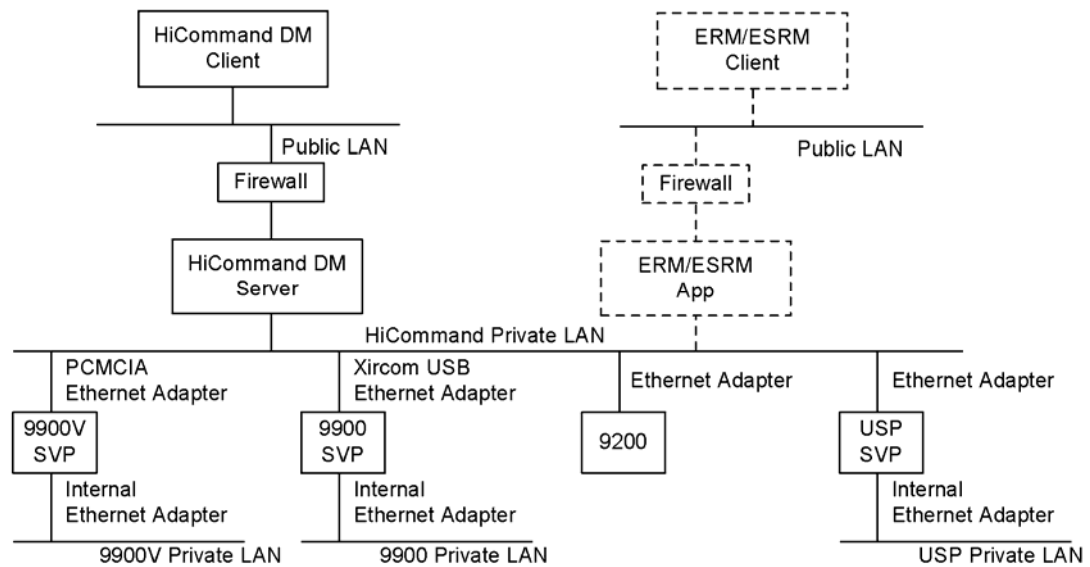


Figure 2.2 Most Secure Configuration: Separate Management LAN Plus Firewall

2.3.2 Second-Most Secure Configuration: Separate Management LAN plus Firewalled Devices under Management

In this configuration, the server hosting Device Manager Server and all other management servers may be single-homed, and the actual devices under management are separated from Device Manager by a firewall. The firewall's rules restrict access to the arrays to Device Manager Server and any other required management application. Management clients accessing Device Manager are not allowed to pass traffic through the firewall to directly talk to the managed arrays, but can participate in management operations directly with Device Manager or the management application.

This configuration is the second most secure, and is more flexible than the most secure option. While this configuration protects the devices under management, it does not protect the management application servers themselves. Therefore, all management application servers should be hardened to the maximum possible extent

Note: A Device Manager client and the storage subsystem must be set so that they can communicate with each other via TCP/IP.

Figure 2.3 illustrates a separate management LAN plus firewalled devices under management.

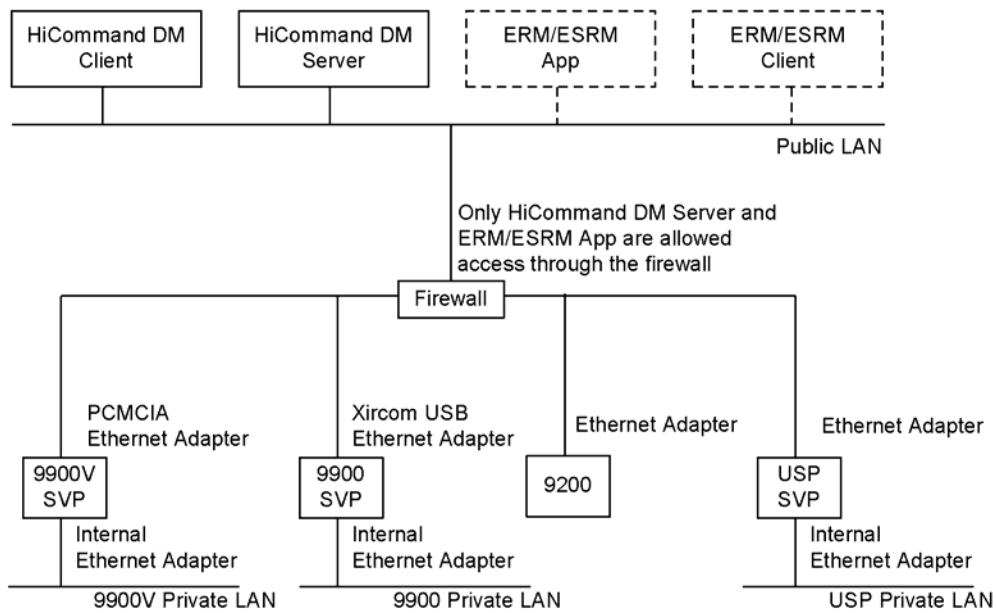


Figure 2.3 Second-Most Secure Configuration: Separate Management LAN plus Firewalled Devices

2.3.3 Third-Most Secure Configuration: Dual-Homed Management Servers plus Separate Management LAN

In this configuration, the management servers themselves act as the intersection point between the management LAN and a production LAN. The server running Device Manager or management applications is dual-homed. One NIC is attached to the management LAN along with the devices under management, and the second NIC is attached to a production LAN along with the management clients (e.g., the Device Manager GUI). Because the management application servers actually act as the gateway between the production LAN and the management LAN, and there is no additional firewall, you must be very sure that the server itself will not route traffic between the two networks.

This configuration is the third most secure, and is more flexible than either the most or second-most secure configurations. While it protects the devices under management, it does not protect the management application servers themselves. Therefore, all management application servers should be hardened to the maximum possible extent. Additionally, because the management application servers themselves act as gateways between the two LANs, OS hardening is very important.

Note: A Device Manager client and the storage subsystem must be set so that they can communicate with each other via TCP/IP.

Figure 2.4 illustrates dual-homed management servers plus a separate management LAN.

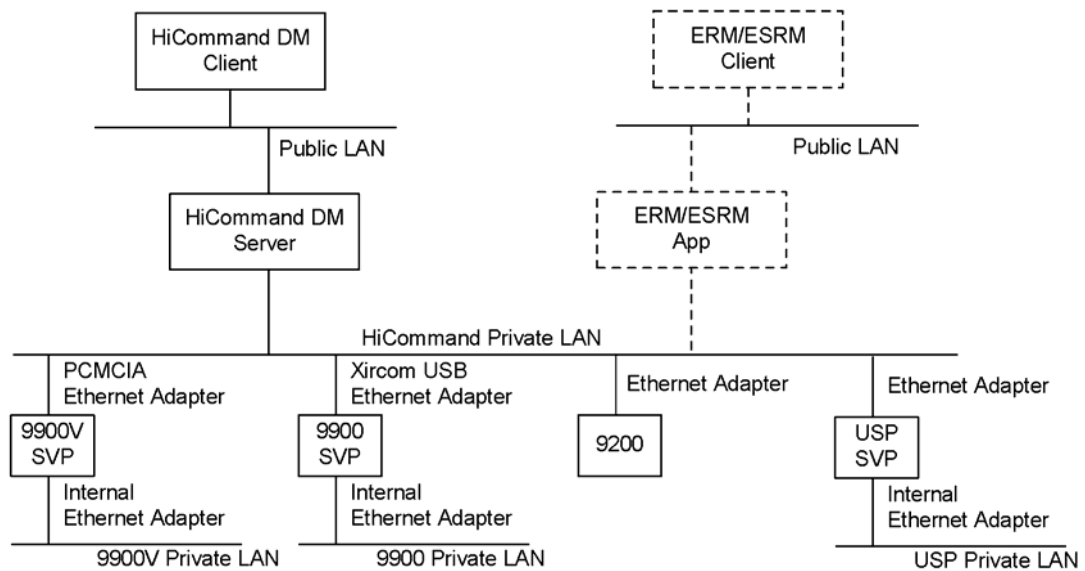


Figure 2.4 Third-Most Secure Configuration: Dual-Homed Management Servers Plus Separate Management LAN

2.3.4 Least Secure Configuration: Flat Network

Here, the management application servers, managed devices, and managed clients all coexist on the same network.

This configuration is the least secure, though it is the most flexible. It affords no protection to any of the components required for storage management operations, so management application server hardening is paramount. Additionally, you should consider microcode updates to any of the devices under management, especially if they are related in any way to security for the device management controllers themselves.

Note: This configuration may be a requirement if the implementation cannot accommodate a management LAN. For example, if you intend to use HDvM Client to launch the physical view of a USP/NSC TagmaStore, you must use a flat network configuration. In other configurations, differences between public and private LANs prevent HDvM from launching Storage Navigator on a client machine.

Figure 2.5 illustrates a flat network.

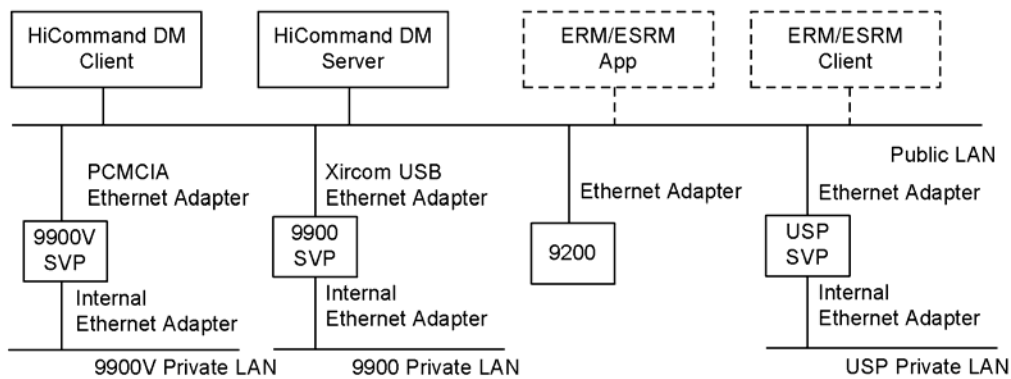


Figure 2.5 Least-Secure Configuration: Flat Network

2.4 Working With a Network That Uses a Firewall

If the host, storage subsystem, management client, and CIM client that are to be managed by the management server are inside a firewall, set the firewall so that these objects can communicate through each port with the management server. Table 2.1 to Table 2.6 list the port numbers relevant to this firewall setting.

A pound sign # next to a port number in these tables indicates that the port number can be changed.

Table 2.1 Ports Used for Communication Between the Management Server and a Management Client

Port number	Originator	Destination	Remarks
23015/tcp#	Management client (Web Client)	Management server	This setting is required when non-SSL communication is used.
23016/tcp#	Management client (Web Client)	Management server	This setting is required when SSL communication is used.
2001/tcp#	Management client (Web Client or CLI)	Management server	This setting is required when non-SSL communication is used.
2443/tcp#	Management client (Web Client or CLI)	Management server	This setting is required when SSL communication is used.
1099/tcp	Management client (Web Client)	Management server	This setting is required for linking with Storage Navigator Modular (for Web) or with DAMP (for Web).

Table 2.2 Ports Used for Communication Between the Management Server and a Managed Host

Port number	Originator	Destination	Remarks
24041/tcp [#]	Management server	Managed host	When the managed host is a mainframe host, this setting is not required.
24042/tcp [#]	Management server	Managed host	n/a
2001/tcp [#]	Managed host	Management server	When the managed host is a mainframe host, this setting is not required.

Table 2.3 Ports Used for Communication Between Management Server and Storage Subsystems

Port number	Originator	Destination	Remarks
21/tcp	Management server	▪ Lightning 9900 ▪ Lightning 9900V ▪ TagmaStore USP	n/a
20/tcp	▪ Lightning 9900 ▪ Lightning 9900V ▪ TagmaStore USP	Management server	Set the firewall so that communication can be established from 20/tcp port of the storage subsystem to any port of the management server.
161/udp	Management server	Lightning 9900	n/a
162/udp	▪ Lightning 9900 ▪ Lightning 9900V ▪ TagmaStore USP	Management server	n/a
1099/tcp	Management server	▪ Lightning 9900V ▪ TagmaStore USP ▪ Thunder 9200 ▪ Thunder 9500V ▪ TagmaStore AMS/WMS series	n/a
51099/tcp	Management server	▪ Lightning 9900V ▪ TagmaStore USP	n/a
2000/tcp [#]	Management server	▪ Thunder 9200 ▪ Thunder 9500V ▪ TagmaStore AMS/WMS series	This setting is required for linking with Storage Navigator Modular (for Web) or with DAMP (for Web).
80/tcp	Management server	Sun T3	n/a

Table 2.4 Ports Used for Management Server to CIM Client Communication

Port number	Originator	Destination	Remarks
427/tcp	CIM client	Management server	n/a
5988/tcp [#]	CIM client	Management server	This setting is required when non-SSL communication is used.
5989/tcp [#]	CIM client	Management server	This setting is required when SSL communication is used.

If there is a firewall between the management client (Web Client) and a storage subsystem, set the firewall so that the following port can be used to perform communication between them.

Table 2.5 Port Used for Communication Between the Management and Mail Servers

Port number	Originator	Destination	Remarks
25/tcp	Management server	Mail server configured to send error information for the storage subsystems by using Storage Navigator Modular (for Web) or DAMP (for Web).	This setting is required when the e-mail error report function is enabled while Device Manager is connected to Storage Navigator Modular (for Web) or DAMP (for Web).

Table 2.6 Port Used for Management Client to Storage Subsystem Communication

Port number	Originator	Destination	Remarks
2000/tcp [#]	Management client (Web Client)	- Thunder 9200 - Thunder 9500V - TagmaStore AMS/WMS series	This setting is required for linking with Storage Navigator Modular (for Web) or with DAMP (for Web).
1099/tcp	Management client (Web Client)	- Lightning 9900V - TagmaStore USP	n/a
80/tcp	Management client (Web Client)	- Lightning 9900V - TagmaStore USP	n/a
51099/tcp	Management client (Web Client)	- Lightning 9900V - TagmaStore USP	n/a

2.5 Registering Firewall Exceptions in a Linux Environment

There is no single standardized firewall function provided by the OS in Linux environments, so firewall exceptions are not registered automatically when Device Manager server is installed. In Linux environments, the user must register firewall exceptions manually.

For details on ports to be registered, see section 2.4.

2.5.1 Using the Text Mode Setup Utility

The following uses an example to explain the procedure for using the text mode setup utility to register a firewall exception.

To register a firewall exception:

1. In a terminal window, execute the `setup` command.
The Choose a Tool window of the text mode setup utility is displayed.
2. Select **Firewall configuration**, use the tab key to move to the **Run Tool** button, and then press **Enter**.
The Firewall Configuration window is displayed.
3. Set **Security Level** to **Enabled** by pressing the space key to select **Enabled**, use the tab key to move to the **Customize** button, and then press **Enter**.
The Firewall Configuration - Customize window is displayed.
4. In **Other ports** specify the port to be registered as an exception, use the tab key to move to the **OK** button, and then press **Enter**.

Example: `Other ports 162:UDP,2001:TCP,23015:TCP`

Important: If a port is already specified, use a comma to separate it from the new added entry.

5. After returning to the Firewall Configuration window, check that **Security Level** is **Enabled**, use the tab key to move to the **OK** button, and then press **Enter**.

Chapter 3 Windows® Systems Installation

This chapter explains how to install the HiCommand Device Manager Server on a Windows system, using the following topics:

- Installation Overview (see section 3.1)
- Installing to a Standard Windows Environment (see section 3.2)
- Installing to a Microsoft Cluster Server Environment (see section 3.3)
- Converting the Database (see section 3.4)
- Verifying and Troubleshooting Installation of HiCommand(R) Device Manager Server and Common Component (see section 3.5)
- Starting and Stopping the Device Manager Server (see section 3.6)
- Operating the HiCommand Device Manager Server Database (see section 3.7)
- Uninstalling the HiCommand Device Manager Server and Related Products (see section 3.8)

3.1 Installation Overview

Instructions in this section are for installing the Device Manager Server software on a single central server system. For instructions on installing and using the graphical Web Client software, see *HiCommand Device Manager Web Client Installation and Configuration Guide*.

WARNING: Device Manager does not support Web Client operations that use Windows terminal service. Device Manager does not support changing the configuration of the HiCommand Device Manager Server and HiCommand Device Manager Agent.

Note: Always read the release notes before installing Device Manager, and make sure that you have the minimum required microcode version on the subsystem.

3.1.1 Windows System and Media Requirements

WARNING: Do not install Tuning Manager version 4.0 or higher on the same server as Device Manager version 4.0 or higher.

WARNING: Do not install Device Manager and Hitachi Storage Services Manager on the same server.

Caution: HiCommand Device Manager does not support operations that use the terminal service function.

Important: The Device Manager Server and Agent must have the same software version to be able to communicate with each other.

Important: Do not install the Device Manager server in a system in which the client environment definitions of HiRDB-related products (e.g., HiRDB/Single Server, HiRDB/Parallel Server, HiRDB/Run Time, HiRDB/Developer's Kit, or HiRDB/Workgroup Server) are set in environment variables.

The following are the minimum suggested requirements for Windows systems:

- Operating System: The HiCommand Device Manager server runs on the following OSs:

Table 3.1 List of Windows Versions on Which HiCommand Device Manager Server Runs

Abbreviated name and service pack	Full name of operating system
Windows 2000 SP3 or SP4 ^{#1}	Microsoft Windows 2000 Professional Operating System
	Microsoft Windows 2000 Server Operating System
	Microsoft Windows 2000 Advanced Server Operating System
	Microsoft Windows 2000 Datacenter Server Operating System
Windows Server 2003 x86 No SP, or SP1 ^{#2#3}	Microsoft Windows Server™ 2003, Standard Edition
	Microsoft Windows Server 2003, Enterprise Edition
	Microsoft Windows Server 2003, Datacenter Edition
Windows Server 2003 x64 Edition No SP ^{#4}	Microsoft Windows Server 2003, Standard x64 Edition
	Microsoft Windows Server 2003, Enterprise x64 Edition
	Microsoft Windows Server 2003, Datacenter x64 Edition
Windows Server 2003 R2 No SP ^{#2#3#4}	Microsoft Windows Server 2003 R2, Standard Edition
	Microsoft Windows Server 2003 R2, Enterprise Edition
	Microsoft Windows Server 2003 R2, Datacenter Edition
Windows Server 2003 R2 x64 Edition No SP ^{#4}	Microsoft Windows Server 2003 R2, Standard x64 Edition
	Microsoft Windows Server 2003 R2, Enterprise x64 Edition
	Microsoft Windows Server 2003 R2, Datacenter x64 Edition
Windows XP SP2 ^{#4}	Microsoft Windows XP Professional

#1 To operate in a cluster environment, SP4 is required.

#2 Only x86 versions are supported.

#3 Also supported on VMware ESX Server 2.5.

#4 Installation using Remote Desktop is only supported for connection with a console session.

- Machine specifications: The following table describes the recommended specifications for the machine where the HiCommand Device Manager server is to be installed.

Table 3.2 Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed

Item	Minimum	Recommended
Processor	1.0 GHz	2.0 GHz or faster
Memory	512 MB	At least 1 GB [#]
Disk space	4 GB	At least 5 GB

When the HiCommand Device Manager server is used concurrently with other software products, the memory requirements of all of the software products must be taken into account.

- Installation destination and its disk space requirements: The following table describes the installation paths and the required disk space for installation.

Table 3.3 Installation Path and Required Disk Space

Item	Default installation path	Required disk space (GB)
Installation destination for the HiCommand Device Manager server	C:\Program Files\HiCommand\DeviceManager ^{#1}	1.30
Installation destination for HiCommand® Suite Common Component	C:\Program Files\HiCommand\Base ^{#2}	
Storage destination of the database for the HiCommand Device Manager server	C:\Program Files\HiCommand\DeviceManager\HiCommandServer\database ^{#1}	0.10
Storage destination of the database for HiCommand Suite Common Component ^{#3}	C:\Program Files\HiCommand\Base\database ^{#1}	1.20
A temporary folder ^{#4}	A folder specified by the environment variable TMP	0.30 ^{#5}

#1 You can change this path.

#2 You can change this path. If you install the HiCommand Device Manager server later, install it in the same drive as this path indicates.

#3 This is not required if HiCommand Suite Common Component version 4.0 or later has already been installed.

#4 This is temporarily required during installation. However, this will be unnecessary after finishing installation.

#5 When the free disk space of the folder specified by the environment variable `TMP` is less than 200 MB, you will be asked to specify another folder during installation. In this case, the drive you specified must have 200 MB of free disk space and the drive of the folder specified by the environment variable `TMP` must have 100 MB of free disk space.

- Prerequisite program: J2SE Java Runtime Environment 1.4
This program is automatically installed when you install the HiCommand Device Manager server.
- Monitor: XGA (1024 x 768 resolution) or higher
- CD-ROM drive
- 10/100 Ethernet LAN card (if the machine and the LAN cable are compatible with Gigabit Ethernet, you can use a Gigabit-class card).
- Static IP address
- Storage subsystem(s) and the Device Manager Server residing on the same network
- Administrator/root ID to install Device Manager
- TCP/IP installed and running
- LAN cables and connections to the subsystem
- The HiCommand Device Manager server only supports IPv4 (it does not support IPv6). Connect the HiCommand Device Manager server, Web Client, the HiCommand® Device Manager agent, and a storage subsystem by using IPv4. For details about how to disable IPv6, refer to the appropriate documentation for each OS.
- The following table shows the number of resources that can be managed by the HiCommand Device Manager server. We recommend that you operate the HiCommand Device Manager server within these limits. The default values in the table are used if you do not change the operation environment settings (the memory heap size settings) of HBase Storage Mgmt Web Service.

Table 3.4 Maximum Value of the Number of Resources that Can Be Managed by the HiCommand Device Manager Server

Resource		When using report function		When not using report function	
		Maximum value for the entire Device Manager	Maximum value for one storage subsystem	Maximum value for the entire Device Manager	Maximum value for one storage subsystem
Number of LUNs	Maximum setting	20,000	20,000	100,000	32,000
	Default	15,000	15,000	32,000	32,000
Number of Securities	Maximum setting	30,000	30,000	150,000	48,000
	Default	20,000	20,000	48,000	48,000
Number of LDEVs	Maximum setting	10,000	10,000	50,000	16,000
	Default	7,500	7,500	16,000	16,000

In an environment in which HiCommand(R) Device Manager is used, if the assumed number of resources exceeds the default setting, estimate the number of managed resources by using the formula shown below. When multiple storage subsystems are to be managed, estimate the number of managed resources for each storage subsystem, and use the greatest value as a guideline.

Formula:

$$\text{number-of-managed-resources} = \text{number-of-LDEVs} \times 2.5 + \text{total-number-of-paths}^{\#}$$
$$\# \text{ total-number-of-paths} = \text{number-of-LDEVs} \times \text{average-number-of-paths-per-LDEV}$$

If the *number-of-managed-resources* is 28,000 or greater or if an *Out Of Memory* error occurs while you are using Web Client to perform an operation such as displaying a list of LDEVs, use the following procedure to set the memory heap size:

Stop the HiCommand Device Manager server and HiCommand Suite Common Component as follows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server with Common Services**.

Execute the following command:

```
"installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsweb" /add /file "installation-folder-for-the-Device-Manager-server\HiCommandServer\webapps\DeviceManager.war" /server HiCommand /javaoption HDvM.serverpath="installation-folder-for-the-Device-Manager-server" /nolog /type DeviceManager /Xms256 /Xmx512
```

The following shows an example of executing the command:

```
"C:\Program Files\HiCommand\Base\bin\hcmdsweb" /add /file "C:\Program Files\HiCommand\DeviceManager\HiCommandServer\webapps\DeviceManager.war" /server HiCommand /javaoption HDvM.serverpath="C:\Program Files\HiCommand\DeviceManager" /nolog /type DeviceManager /Xms256 /Xmx512
```

Restart the HiCommand Device Manager server and HiCommand Suite Common Component as follows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Start Server with Common Services**.

When using one HiCommand Device Manager server, it is not possible to use separate storage partitions with different storage administrator accounts. If you want to manage individual storage partitions, a HiCommand Device Manager server is required for each storage partition.

Caution: If CIM/WBEM functions are being used, you might have to increase the memory heap size, depending on the conditions.

To change the memory heap size:

1. Edit the `HiCommandServer.lax` file in the following folder to change the memory heap size:
installation-folder-for-the-Device-Manager-server\HiCommandServer
2. Open the `HiCommandServer.lax` file in a text editor, and change the value of `lax.nl.java.option.java.heap.size.max` to *new-setting-value* (units: bytes) in the formula below. Note that if the value of *calculation-value-for-SMI-S-Provider* is smaller than 268,435,456 bytes (256 MB), use 268,435,456 bytes (256 MB) as the value of *calculation-value-for-SMI-S-Provider*, and then calculate the value of *new-setting-value*.

calculation-value-for-SMI-S-Provider = 30000 x *number-of-LDEVs* x *number-of-paths*

new-setting-value = *current-setting-value* + *calculation-value-for-SMI-S-Provider*

3. After the `HiCommandServer.lax` file is changed, perform the following to restart the Device Manager server.

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.

After the Device Manager server has stopped, select **Start, Programs, HiCommand, Device Manager**, and then **Start Server**.

Caution: Depending on the language of the installed OS (such as German or Spanish) on the installation destination Windows machine, the installation files and directories of the Device Manager server might be viewed, deleted, and operated by users who do not have Administrator privileges. (This problem does not occur in an English environment.) Regardless of the language of the installed OS, after installing Device Manager, do not manually delete or operate files or directories.

3.2 Installing to a Standard Windows Environment

The estimated installation time is 30 minutes, for a new installation on a machine configured as follows:

- OS: Windows 2000 SP4
- Processor: Pentium® 4 (2.4 GHz)
- Memory: 1 GB

For Windows XP SP2 or later, or Windows Server 2003 SP1, the installation time requires approximately 15 more minutes, because the HiCommand Device Manager server is added to the Windows firewall exceptions list during the installation.

3.2.1 Preparing for Installation

The Device Manager Server is installed to:

c:\program files\HiCommand\Device Manager

The Common Component is installed to:

c:\program files\HiCommand\Base

Note: Always read the Release Notes before installing Device Manager, and make sure that you have the minimum required microcode version on the subsystem.

Caution: If Windows Firewall is enabled in Windows Server 2003 SP1 or Windows XP SP2, during installation, a warning dialog box might be output asking you whether you want to keep blocking the program. If it appears, choose **Unblock** or **Ask Me Later**. Also, after installation finishes, you need to set up Windows Firewall.

The Device Manager Server installation CD includes the following applications:

- Java 2 Java Runtime Environment (JRE)
- HiCommand Suite Common Component software
- Device Manager Server software
- HiRDB/EmbeddedEdition_HD0 version 7.0

After these products are installed, the Device Manager Web Client software can be downloaded, installed, and updated on the client system from the Device Manager Server. For more information on using the Device Manager Web Client, please see the *HiCommand Device Manager Web Client User's Guide*.

Before you start installation, check the usage status of the port numbers, the installation status of other programs, and other information as described below.

3.2.1.1 Check Port Numbers

Check whether the port numbers required to use HiCommand Device Manager are being used by another product on the machine on which the HiCommand Device Manager server is to be installed by using the `netstat` command.

Example: Check whether another program is using the port 162/udp.

Execute the following command:

```
> netstat -anp UDP
```

Active Connections

Proto	Local Address	Foreign Address	State
UDP	gone:portmap	*:*	
UDP	gone:445	*:*	
UDP	gone:sytek	*:*	

In the command execution results, if there are no lines in which UDP for Proto, 162 for Local Address, and LISTENING for State appears, the port is not being used.

Also, make sure that the following file does not contain a 162/udp description:

%SystemRoot%\system32\drivers\etc\services

Replace %SystemRoot% with the value of the Windows environment variable SystemRoot.

The following shows the ports required to use HiCommand Device Manager. For details about the intended use of each port, see section 2.4 and section 5.4.1.

Port numbers that must be checked

- From 23015 to 23018, and 23032: If another product is using any of these ports, change the settings of that product, or change the settings of HiCommand Device Manager. For details about how to change these port numbers, see section 5.4.2. If HiCommand Suite Common Component has been installed and these ports have been changed, you can install the HiCommand Device Manager server by using those ports. You do not need to set up the default ports.
- From 45001 to 49000: For these port numbers, the settings of HiCommand Device Manager cannot be changed. Therefore, you need to change the settings of any other products that are using the same ports as HiCommand Device Manager.
- 2001: If another product is using this port number, change the settings of that product, or change the port number to be used before HiCommand Device Manager starts. For details about how to change this port number, see section 8.2.2. We recommend that you change this port number to another number because this port number is included among the port numbers temporarily assigned by Windows (1024 to 5000). If another product is using this port number, HiCommand Device Manager will not be able to start, and the following message will be output to the application log and sys log: KAIC00114-E An attempt to start the HTTP server on port "2001" failed.

Port numbers that must be checked when some functions are enabled

- 162: This port number is used when the SNMP Trap reception function of HiCommand(R) Device Manager is enabled. To disable the SNMP Trap reception function, select disable in the Setting for the SNMP Trap Reception Function panel during installation.
- 1099: This port number is used when the function to link with Storage Navigator Modular (for Web) (see section 9.1), or DAMP (for Web) (see section 9.1.4) is enabled. We recommend that you change this port number to another number because this port number is included among the port numbers temporarily assigned by Windows (1024 to 5000). For details about how to change the port number used to link with Storage Navigator Modular (for Web), see section 9.1.2. The port number for the function to link with DAMP (for Web) cannot be changed. When the port number 1099 is used by another product, perform one of the following operations so that other products do not use the port number 1099 at the same time as HiCommand Device Manager.

If a product that uses the port number 1099 is always running, use different machines to run HiCommand Device Manager and that product respectively.

If a product that uses the port number 1099 runs temporarily, restart DAMP (for Web).

- 2000: This port number is used when the function to link with Storage Navigator Modular (for Web) (see section 9.1) or DAMP (for Web) (see section 9.1.4) is enabled. For details about how to change this port number, see section 1.5.1.1 or 1.5.1.5. We recommend that you change this port number to another number because this port number is included among the port numbers temporarily assigned by Windows (1024 to 5000).

- 2443: This port number is used when SSL communication is enabled. For details about how to change this port number, see section 8.2.3. We recommend that you change this port number to another number because this port number is included among the port numbers temporarily assigned by Windows (1024 to 5000). If another product is using this port number, the following message will be output to the application log and sys log and HiCommand Device Manager will not be able to start:
KAIC00115-E An attempt to start the HTTPS server on port "2443" failed.

3.2.1.2 Check Other Programs Related To Security

- Check whether the following programs are installed. If they are installed, take action by following the explanation below:
 - A program that monitors security
Stop the program that monitors security, or change its settings so that Device Manager can be installed normally.
 - A program that detects viruses
We recommend that you stop programs that detect viruses, and then install Device Manager.

If a program that detects viruses is running during installation of Device Manager, the speed of installation might be reduced, installation might fail, or installation might finish in an incorrect state.
 - A program that monitors processes
Stop the program that monitors processes, or change its settings so that the program does not monitor the services or processes of the HiCommand Device Manager server and the HiCommand Suite Common Component.

If a program that monitors processes starts or stops the above services or processes during installation of Device Manager, installation might fail.
- For Windows Server 2003 SP1 and Windows XP SP2, disable Data Execution Prevention before starting the installer.

To disable Data Execution Prevention:

1. Log in to the system using a user ID with Administrator permissions.
2. Insert the HiCommand Device Manager installation CD-ROM.
3. From Control Panel, choose **System**.
The Properties dialog box for the system appears.
4. Choose the **Advanced** tab, and then click the **Settings** button under **Performance**.
The Performance Options dialog box appears.
5. Choose the **Data Execution Prevention** tab, and then select the radio button for **Turn on DEP for all programs and services except those I select**.
6. Click the **Add** button.
The dialog box for choosing a file appears.

7. Choose `install.exe` in the root folder of the CD-ROM drive, and then click the **Open** button.
8. Click the **OK** button.

3.2.1.3 Check Other Programs

- HiRDB Embedded Edition_HD0 must be always running when you are using any HiCommand Suite products version 4.0 or later. You can verify that HiRDB is running by checking the Services Panel.
- Open the property of the following services from the Services panel to make sure that **Startup Type** is not set to **Disabled**. If **Startup Type** is set to **Disabled**, change the setting to **Automatic** or **Manual**.
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiRDB/EmbeddedEdition_HD0
 - HiCommandServer
- Device Manager cannot be installed on a server on which Tuning Manager has been installed in a Large configuration. Trying to install Device Manager in such an environment will automatically cancel the installation. If that happens, install Tuning Manager and Device Manager separately on different servers.
- You cannot install a version of Tuning Manager earlier than 4.0 on a machine on which Device Manager 4.0 or later has been installed. The following installation sequences are allowed:
 - Device Manager 4.0 or later is installed after a version of Tuning Manager earlier than 4.0 has been installed.
 - Tuning Manager 4.0 or later is installed after a version of Device Manager earlier than 4.0 has been installed.
- If you are using another HiCommand Suite product, make sure that you back up the databases for that product before installing Device Manager. For details about how to back up other HiCommand Suite product databases, see the manual for each product.
- The HiCommand Device Manager server cannot coexist with the following HiRDB products. Therefore, do not install the Device Manager server on a machine on which any of the following HiRDB products are installed, or vice-versa.
 - HiRDB/Single Server
 - HiRDB/Parallel Server
 - HiRDB/Workgroup Server
 - HiRDB/Run Time
 - HiRDB/Developer's Kit
 - HiRDB SQL Executer

3.2.1.4 Check Other Information

- Make sure no other applications are running.
- The user's account must be a member of the Administrator group.
- Make sure that the following folders can be created, or that they have already been created and are write-enabled. The examples assume that the OS is on the C Drive, and that Device Manager is installed to the default installation folder.
 - C:\Program Files\HiCommand
 - C:\Program Files\Hitachi\HNTRLib2
 - C:\Program Files\Common Files\Hitachi
- You cannot perform a downgrade installation for Device Manager. For example, in an environment in which Device Manager 5.0 has been installed, you cannot install Device Manager 4.3 or an earlier version. However, a build to which patches have been applied can be overwritten by the same build without the patches, as long as the version numbers are the same. For example, after installing a build of Device Manager 5.0 to which patches have been applied, you can install a V5.0 build that does not contain the patches.
- When you specify virtual memory settings, allocate at least 1,536 MB as the paging file size. To set the paging file size, right-click **My Computer** and, in the displayed menu, choose **Properties**. Then, in the displayed dialog box, open the **Advanced** page and click **Performance Options**. The allocated paging file size must be at least 1,536 MB even after Device Manager server operation starts.

3.2.2 Performing a New Installation of Device Manager Server

After finishing a new installation, be sure to back up the Device Manager Server database.

To perform a new installation of the Device Manager Server:

WARNING: Close the Services panel before you install the HiCommand Device Manager server.

1. Log on to the system as an administrator.

If a user that is not from the administrators group attempts installation, a window is displayed indicating that the user must be from the administrators group to perform installation. The installation then stops.
2. Because this is a new installation, you should not have any Device Manager components currently installed. Stop any other HiCommand Suite product that is running.
3. Load the Device Manager installation CD-ROM. From the **Start** menu, select **Run**, and then **Browse**. Navigate to the CD folder and select **install.exe** from the list of root files.
4. The panel for choosing the language displays. Select the appropriate language, and then select **OK** to continue.

The following steps assume that English is selected.
5. The **Introduction** panel displays. Select **Next** to continue.

6. When the HiCommand Suite Common Component services are running, the **Stop HiCommand Suite Common Component Services** panel is displayed. Select **Next** to continue.

If the installer cannot stop the HiCommand Suite Common Component services, the **HiCommand Suite is running** panel is displayed, meaning you cannot continue installation. In that event, select **Cancel**, stop any HiCommand Suite products manually, and then re-start the installation.
7. The **Backup recommendation** panel is displayed. If a HiCommand Suite product other than Device Manager is installed, you should back up the databases for HiCommand Suite Common Component and other HiCommand Suite products before starting an installation. Otherwise, select **Next** to continue.
8. If Common Component is not installed, the **HiCommand Suite Common Component Not Installed** panel is displayed. Select **Next** to continue.
9. If port 162 is not used by any other products, the **SNMP Trap Note** panel displays. Select **Next** to continue.
10. If another product is using port 162, the **Setting for the SNMP Trap Reception Function** panel is displayed. If the SNMP Trap reception function is enabled when another product is using port 162, Device Manager will not start after installation. If you want to disable the SNMP Trap reception function to start Device Manager, choose **YES. Disable the function and continue installation**, and then **Next** to continue. If you want to change the settings of the product that is using port 162 and re-execute the installation, choose **NO. Stop the installation of Device Manager**, and then **Next** to cancel the installation.

Caution: If you choose **YES. Disable the function and continue installation**, the properties for the SNMP Trap reception function are automatically changed to disable the function. You must reset these properties to the default values manually. For details about these properties, see section 8.5.8.
11. The **Choose Install Folder** panel displays. To accept the default folder, select **Next**. To change to another install folder, make that selection and then select **Next**.

Caution: Specify an absolute path, using no more than 64 bytes. Do not enter the path delimiter (\) at the end of the folder path. Space characters and the following characters can be used for the path:

A-Z a-z 0-9 . _ ()

The path cannot contain consecutive spaces. Folder names must not end with a period or space. Do not use parentheses, except when referring to Program Files (x86) folder.
12. The **Install Folder Information** panel is displayed. Select **Next** to continue.

Important: When the Common Component 4.0 or later is being installed, HiRDB is installed to manage the database. No dialogue box is displayed during the HiRD8 installation.
13. The **Choose the Database for HiCommand Suite Common Component** panel is displayed (see Figure 3.2). Specify the location where the database files used by HiCommand Suite Common Component are to be stored, in accordance with the following limitations:
 - Specify an absolute path, using no more than 90 bytes.

- Do not enter a path delimiter (\) at the end of the folder path.
 - You can use alphanumeric characters, spaces, underscores and periods for the path name.
 - Folder names must not end with a period or space.
14. Select **Next** to continue. The **Choose the Database for HiCommand Device Manager** panel is displayed (see Figure 3.3).
 15. Specify the file location for the Device Manager Server. The file name and path have the same restrictions as the Common Component file name and path. Select **Next** to continue.
 16. The **Installation Server Information Settings** panel displays (see Figure 3.4). Enter the IP address or host name of the server machine, and the port number for the HBase Storage Mgmt Web Service used by Web Client, then select **Next**. The defaults are as follows:
 - IP address or host name: Default = None. Specify a valid host name or IP address on the network on which HiCommand Device Manager operates.
 - Port number: Default = 23015.

Important: This is the port number for the HBase Storage Mgmt Web Service used by Web Client, not the Device Manager Server. If you use a port number other than the default, make sure that you also change the port number assigned to the Common Component. See section 5.4.2 for more information on changing Common Component ports.
 17. If a Windows Firewall is installed on the system, the **Adding to the Windows Firewall Exceptions** panel is displayed. Check the contents of the panel, and select **Next** to continue.
 18. The Setting for the SMI-S Provider Service panel is displayed (see Figure 3.5). If you want the SMI-S Provider service to start automatically when Device Manager starts, choose **YES. Automatically enable the function after installation**. If you do not want it to start automatically, choose **NO**. Then, choose **Next** to continue.

If you chose **YES. Automatically enable the function after installation**, set up the options by following the instructions in steps 18 and 19. If you chose **NO**, go to step 20.

Note: You can set up the SMI-S Provider service after installation. For details, see Chapter 11.
 19. The Setting for the SMI-S SSL panel is displayed (see Figure 3.6). To enable SSL for the SMI-S Provider service, choose **YES**. To disable SSL, choose **NO**. To change the port number, enter the new port number in the **Change the port number if needed** text box. To enable two-way authentication for SSL-based object operations, select **Also use Two-way Authentication for Object operations**. To enable two-way authentication for SSL-based event indications, select **Also use Two-way Authentication for Event Indications**. Select **Next** to continue.

Caution: Two-way authentication involves import and export of authentication files. For details, see section 7.4.

Note: You can enable SSL, change the port number, and set up two-way authentication after installation. For details on the setup procedures, see the following sections:

To enable SSL and change the port number:

Section 11.3.2.2

Section 11.4.1

To set up two-way authentication:

Section 7.4

20. The Setting for the SLP Service panel is displayed (see Figure 3.7). To install and enable the SLP service, choose **YES. Automatically enable the function after installation**. If you do not want to enable the SLP service, or if another SLP service is already installed and enabled, select **NO**. Select **Next** to continue.

Note: You can enable the SLP service after installation. For details, see section 11.5.

21. The **Pre-installation Summary** panel displays. The product name, installation folder, information on installation disk capacity, the IP address or host name of the server machine, and the port number to be used are displayed. Verify that the information is correct, and then select **Install** to begin.
- If you select **Cancel**, the **Cancellation Warning** panel displays, warning that if you cancel now installation will not complete.
 - If you let installation proceed without cancellation, the **Please Wait** panel displays, followed during post-installation setup by the Progress panel.
22. The **Secure Socket Certificates Note** panel displays.
23. If you plan to run secure socket communications, note the information in this panel for later use. For more information on configuring secure sockets, see Chapter 7. Select **Next** to continue.
24. The **Install Complete** panel displays.
25. Select **Finish** to complete the installation.

Important: After installing the HiCommand Device Manager server, you need to register a license key by using Web Client. For information about how to register a license key, see the *HiCommand Device Manager Web Client User's Guide*.

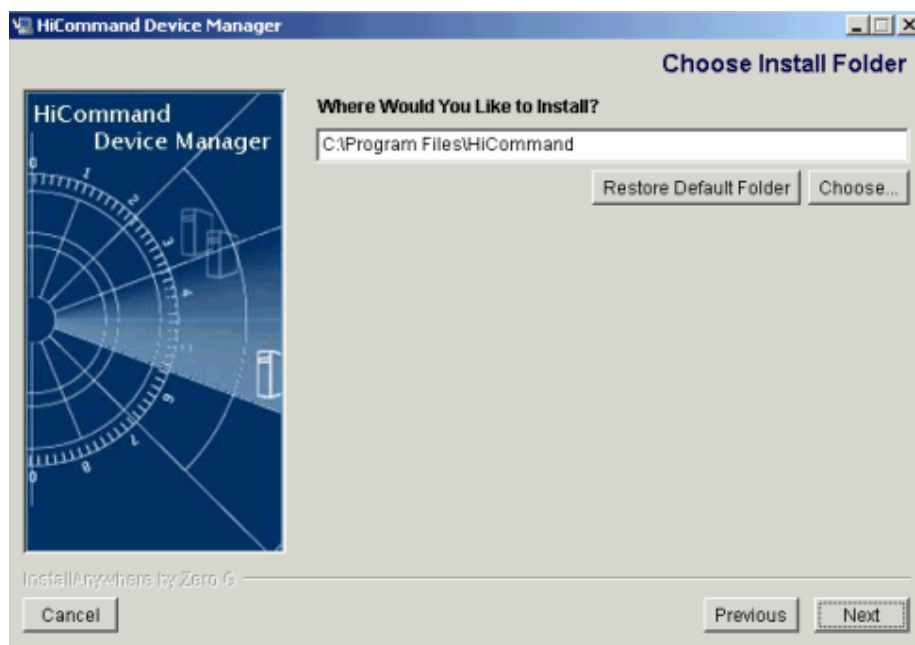


Figure 3.1 Choose Install Folder Panel

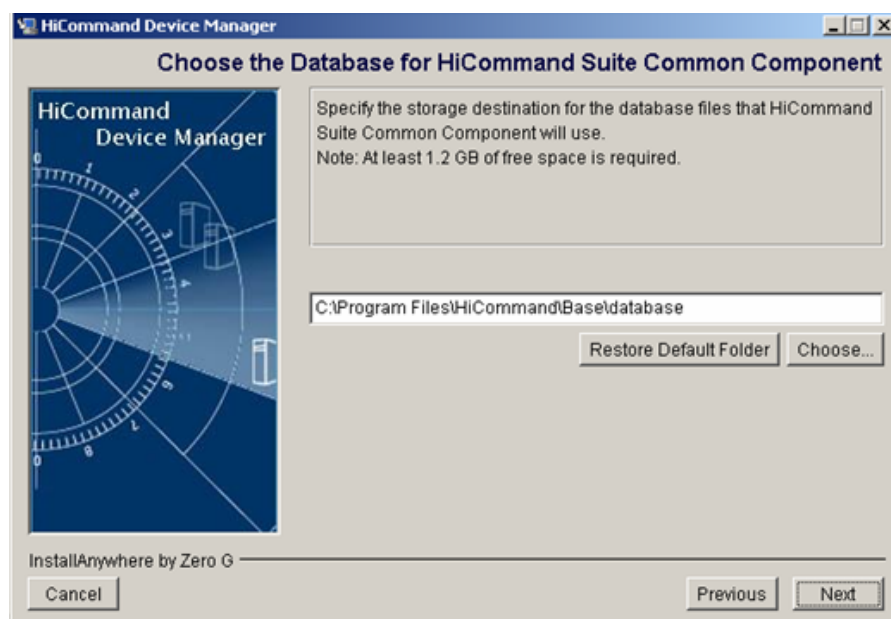


Figure 3.2 Choose the Database for HiCommand Suite Common Component Panel

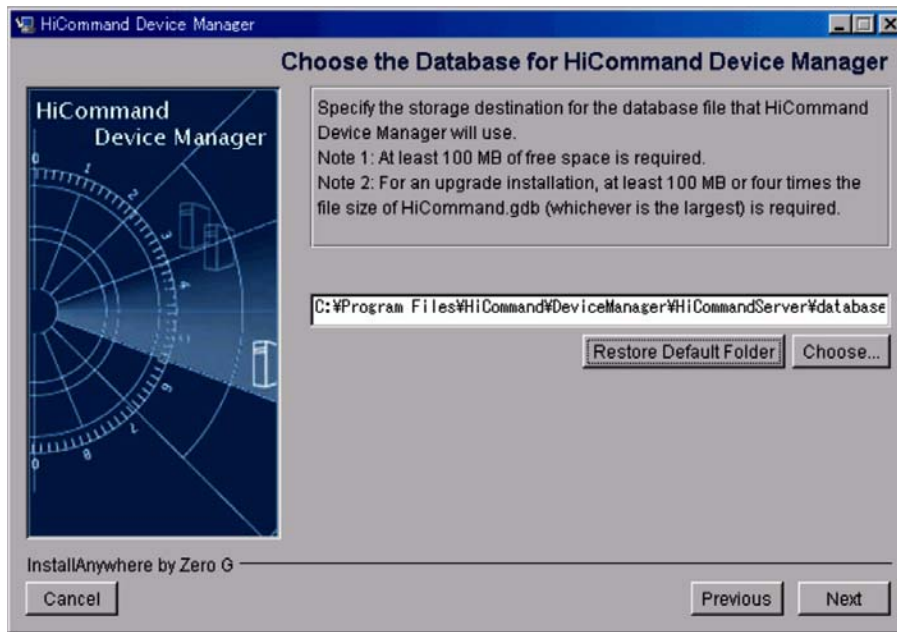


Figure 3.3 Choose the Database for HiCommand Device Manager Panel

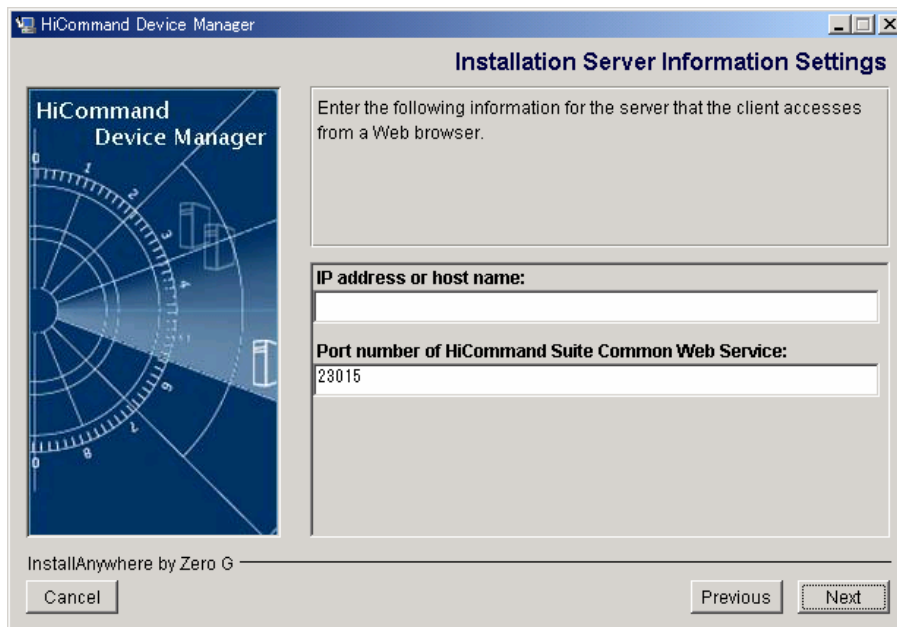


Figure 3.4 Installation Server Information Settings

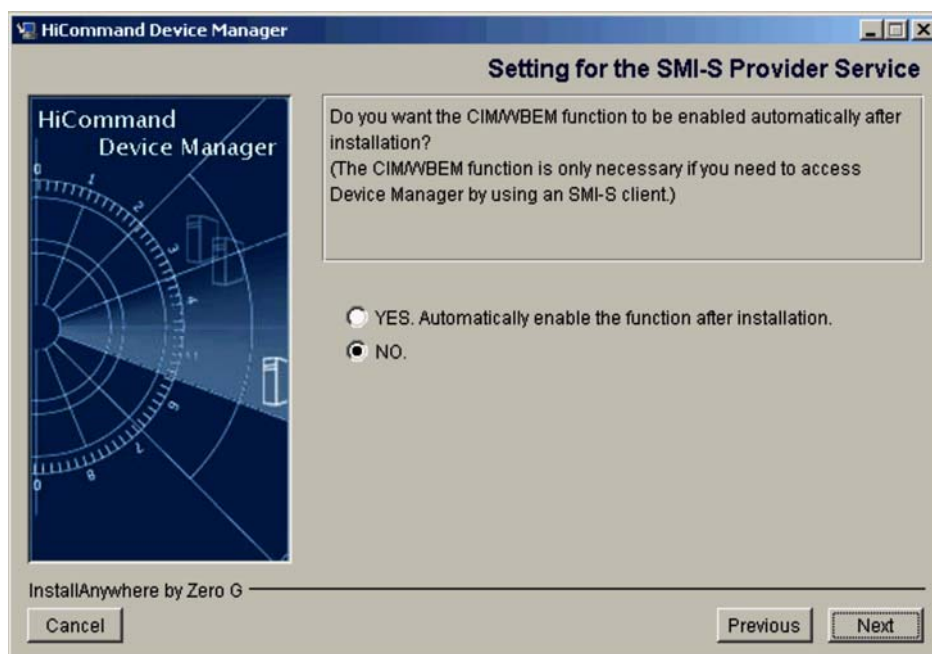


Figure 3.5 Setting for the SMI-S Provider Service Panel

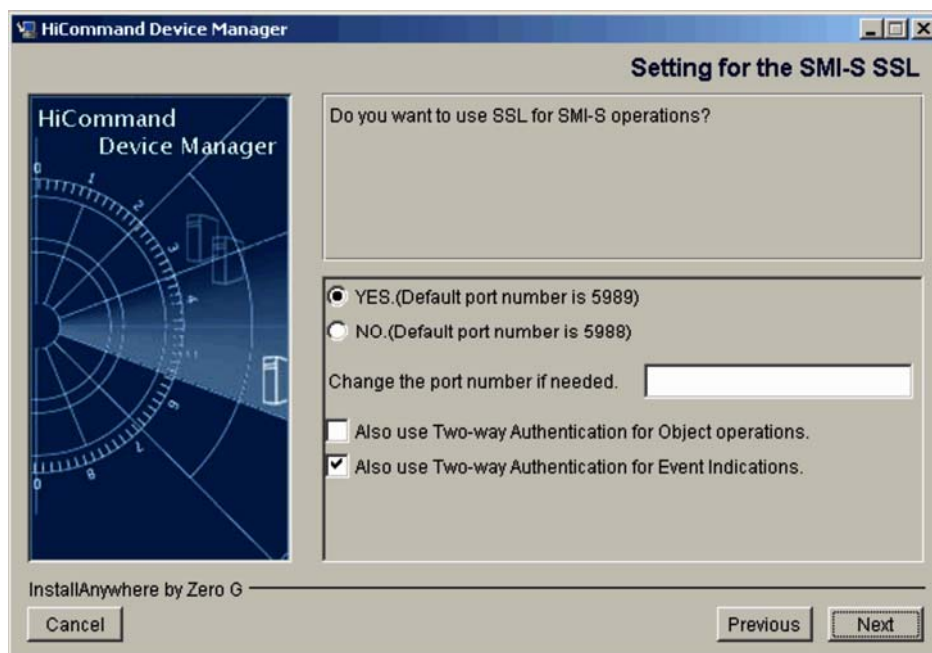


Figure 3.6 Setting for the SMI-S SSL Panel

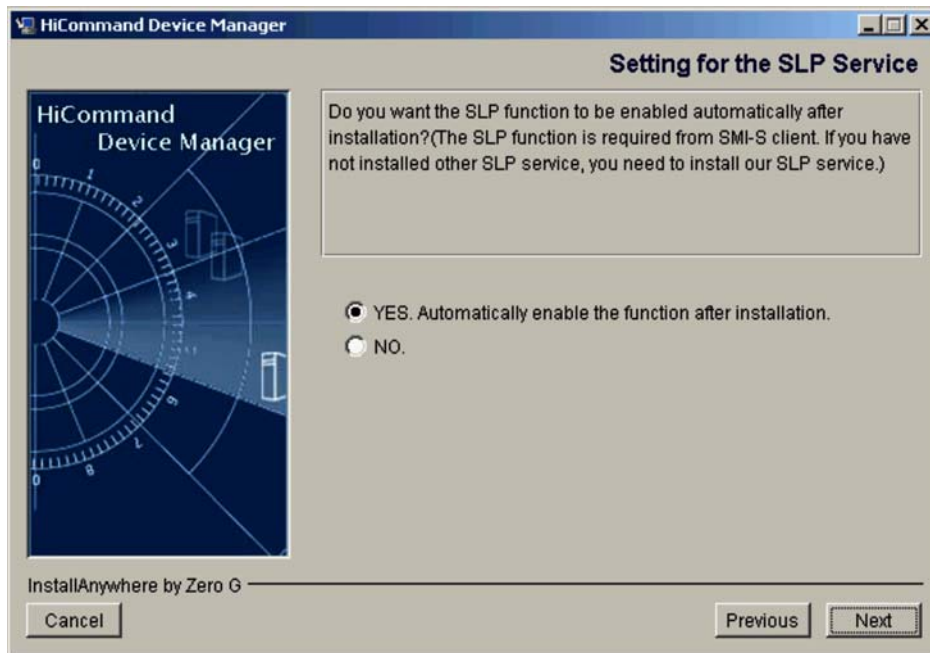


Figure 3.7 Setting for the SLP Service Panel

3.2.3 Performing an Upgrade Installation from Version 3.5 or Earlier

After finishing an upgrade installation, be sure to back up the Device Manager Server database.

3.2.3.1 About Upgrades

WARNING: Close the Services panel before you upgrade the HiCommand Device Manager server. Otherwise, the HiCommand Device Manager server service will be deleted when you close and then re-open the Services panel.

Device Manager will be installed in:

c:\program files\HiCommand\Device Manager

The Common Component will be installed in:

c:\program files\HiCommand\Base

WARNING: Do not cancel in the middle of an upgrade or re-installation, because you could corrupt the files.

WARNING: If you are updating the Common Component data base and an error occurs and auto-recovery fails, you must manually recover the database before you re-install the server. Once you upgrade or re-install the server, you will not be able to recover the Common Component database. To find a database update error, check the following log file: **<installation directory>\Base\log\hcmdsdbupdate.log**. You will want to restore the file named **<installation directory>\Base\database\hbase_vup_back.gbk**. For instructions on how to restore the Common Component database, see section 3.3.4.

WARNING: If either InterBase or InterServer have previously been installed, that service must be running when you upgrade the Device Manager Server.

WARNING: Do not re-install Device Manager when the Control Panel Service window is open.

WARNING: If you have made any changes to **<common component installation folder>\conflinit.conf**, and you are upgrading from Device Manager version 3.0 or 3.1 to version 3.5 or later, you must first create a new folder for **<common component installation folder>\confluser.conf**, and duplicate those changes in this file.

Caution: If CIM/WBEM functions are being used when upgrading, you must release the registration of the SLP service from the Windows service before performing the upgrade. For details about releasing an SLP service registration, see the *HiCommand Device Manager CIM/WBEM User's Guide*.

If you have performed an upgrade installation without releasing the SLP service registration, it may fail to launch the SLP service after the installation.

In such a case, do the following:

1. Disable the Service Location Protocol service from the **Service** window in Windows.
2. Restart Windows.
3. Release the SLP service registration.
4. Register the SLP service again.

If you want to install a newer version of the Device Manager Server, install it over the existing version. Device Manager automatically updates your data and configurations to work with the latest version. The previous **HiCommandCLI.properties** file is saved as **HiCommandCLI.properties.old** in the same directory. The previous **TIA.properties** file is saved as **TIA.properties.old** in the same directory.

Important: If the **HiCommandCLI.properties** file contains multiple entries of the same key with different values, the value of the most recently specified key overrides the others. Although key duplication does not affect HiCommand CLI operations, we do not recommend that you specify the same key more than once with different values. We recommend that you eliminate unnecessary duplicate keys and their values. If there are duplicate keys that have different values during an upgrade installation, the new **HiCommandCLI.properties** file will inherit keys as follows:

If there are multiple `password` keys:

All `password` keys and their values in the old **HiCommandCLI.properties** file are written to the new file as is. The following shows an example:

- The `password` keys and their values in the old file:
`password=AAA`
`password=BBB`
- The `password` keys and their values written to the new file:
`password=AAA`
`password=BBB`

If there are duplicate keys other than `password`:

The name and value of the most recent duplicate key in the old `HiCommandCLI.properties` file are written to the new file as many times as there are duplicated keys. The following shows an example:

- The `user` keys and their values in the old file:
`user=AAA`
`user=BBB`
- The `user` keys and their values written to the new file:
`user=BBB`
`user=BBB`

Note: User-created files will not be saved as ***.old** during the upgrade.

Important: The characters that can be used for user IDs in HiCommand Device Manager server (version 3.5 or later) are as follows:

A-Z a-z 0-9 - _ . @ + #.

User IDs containing characters other than the above cannot use version 3.5 or later. Thus, you must re-register users who have user IDs that contain unusable characters. If the User IDs of all the users who have the Admin permissions contain unusable characters, create new users by using the procedure in section 10.1.

Important: The characters that can be used for passwords in version 03-01-/A are as follows:

A-Z a-z 0-9 ! # \$ % & () * + - . = @ \ ^ _ | ' .

If a user cannot log in because their password contains a character other than the above, change the password for that user. If all users are unable to log in, view the procedure in section 10.1 and change the password to a password that contains only usable characters.

3.2.3.2 Upgrading Device Manager Server

Caution: In version 5.0 or later, user information is managed by using the user management functionality of HiCommand Suite Common Component. The registered user information is migrated to the HiCommand Suite Common Component repository when the Device Manager server program is started for the first time after the upgrade installation. For this migration, also note the following points:

- If there is user information that cannot be migrated to the HiCommand Suite Common Component repository due to data corruption or some other problem, that information is output to the Device Manager trace log file.
- If user accounts with the same user ID but different passwords have been registered in both HiCommand Suite Common Component and Device Manager, the user account in HiCommand Suite Common Component overrides the one in Device Manager. The user account registered in Device Manager becomes unavailable, and information to that effect is output to the Device Manager trace log file. For details about the Device Manager trace log file, see section 5.3.1.
- If user accounts that have the same user ID and password have been registered in both HiCommand Suite Common Component and Device Manager, the user account in Device Manager is added to the one in HiCommand Suite Common Component.
- You cannot migrate the user account whose user ID is `System`. The user management functionality of HiCommand Suite Common Component defines this user ID as having the `Admin` permission for all HiCommand Suite products (version 5.0 or later).

WARNING: You cannot upgrade Device Manager version 2.2 or earlier directly to version 4.0 or later. You must first upgrade to a version between 2.3 and 3.5, and then upgrade to version 4.0 or later.

To upgrade the HiCommand Device Manager Server:

1. Log on to the system as an administrator.
If a user who is not from the administrators group attempts installation, a window is displayed indicating that the user must be from the administrators group to perform installation. The installation then stops.
2. Stop any other HiCommand Suite software that is running.
3. Load the HiCommand Device Manager installation CD-ROM. From the **Start** menu, select **Run**, and then **Browse**. Navigate to the CD folder and select `install.exe` from the list of root files.

WARNING: If you attempt to downgrade HiCommand Device Manager, the installer displays the **HiCommand Device Manager Upgrade Error** panel and exits. However, if the version and revision numbers of the builds before and after a downgrade are the same, the installer displays the **WARNING: HiCommand Device Manager Downgrade** panel. If there is no problem, select **Next** to continue.

4. When the HiCommand Suite Common Component services are running, the **Stop HiCommand Suite Common Component Services** panel is displayed. Select **Next** to continue.

If the installer cannot stop the HiCommand Suite Common Component services, the HiCommand Suite is running panel is displayed, and the installation stops. Stop the HiCommand Suite Common Component services manually, and then perform installation again.

To display the **Cancel Installation** panel, choose **Cancel**.

5. The **HiCommand Device Manager Already Installed** panel is displayed. Select **Next** to continue.

6. If the InterBase Not Installed panel or the Incorrect InterBase Version panel is displayed, choose **Cancel** to cancel the installation.

If InterBase 6.0 has not been installed, uninstall the HiCommand Device Manager server and then start a new installation, or install HiCommand Device Manager 3.5 or earlier and then perform an upgrade installation.

If the version of InterBase is incorrect, an upgrade installation cannot be performed. In this case, uninstall the HiCommand Device Manager server, and then start a new installation.

7. If the InterClient Not Installed panel or the Incorrect InterClient Version panel is displayed, choose **Cancel** to cancel the installation.

If InterClient 2.0 has not been installed, uninstall the HiCommand Device Manager server and then start a new installation, or install HiCommand Device Manager 3.5 or earlier and then perform an upgrade installation.

If the version of InterClient is incorrect, an upgrade installation cannot be performed. In this case, uninstall the HiCommand Device Manager server, and then start a new installation.

8. If Common Component 4.0 or later has not been installed, the **Choose the Database for HiCommand Suite Common Component** panel is displayed (see Figure 3.2). Specify the file location for Common Component. Use the following conventions for the path name:

- Specify an absolute path, using no more than 90 bytes.
- Do not enter a path delimiter (\) at the end of the folder path.
- You can use alphanumeric characters and spaces for the path name.
- Folder names must not end with a period or space.

9. Select **Next** to continue. The **Choose the Database for HiCommand Device Manager** panel is displayed (see Figure 3.3).

10. Specify the file location for the Device Manager Server:

- The file name and path have the same restrictions as the Common Component file name and path.

11. Select **Next** to continue. If the Common Component 3.0 or later has not been installed, the **Installation Server Information Settings** panel displays (see Figure 3.4).

12. Enter the IP address or host name of the server machine, and the port number for the HBase Storage Mgmt Web Service used by Web Client, and then select **Next**. The defaults are as follows:

- IP address or host name: Default = None. Specify a valid host name or IP address on the network on which HiCommand Device Manager operates.
- Port number: Default = 23015

Important: This is the port number for the HBase Storage Mgmt Web Service used by Web Client, and not the HiCommand Device Manager server. If you use a port number other than the default, make sure that you also change the port number assigned to the Common Component. See section 5.4.2 for more information on changing Common Component ports.

13. The **Pre-installation Summary** panel displays. The product name, installation folder, information on installation disk capacity, the IP address or host name of the server machine, and the port number to be used are displayed. Verify that the information is correct, then select **Install** to begin.
14. If you select **Cancel**, the **Cancellation Warning** panel will display, warning you that if you cancel now installation will not complete.
WARNING: Choosing cancel after data conversion starts but before installation completes could damage the database.
15. **The Database Conversion** panel (see Figure 3.8) is displayed. When you select **Convert the database during installation**, the installer automatically converts the database:
If the database conversion fails, the Database Convert Error panel (see Figure 3.9) is displayed.
Important: If the upgrade operation is interrupted due to an error before the database conversion finishes, you must take specific recovery action. For instructions, see Chapter 10. Note that It might take a long time to convert the database. For example, if 8,000 LDEVs and 16,000 paths have been managed, the database conversion will take about 5 minutes in an environment that has a 1.5 GHz CPU and 1 GB of memory.
Note: When you select **Next** in this window to display the subsequent window, you cannot return to this window by selecting **Previous** in the subsequent window.
16. When you select **Convert the database** after installation finishes, you will need to manually convert the database. For instructions, see section 3.4.1.
17. The **Please Wait** panel displays, followed by the Progress panel.
18. The Service Startup Finished panel is displayed. Select **Next** to continue.
19. The **Secure Socket Certificates Note** panel. If you plan to run secure socket communications, note the information in this panel for later use. For more information on configuring secure sockets, see Chapter 7. Select **Next** to continue.
20. The **Install Complete** panel displays. Select **Finish** to complete the installation.
21. Refresh all the registered subsystems to update the database.

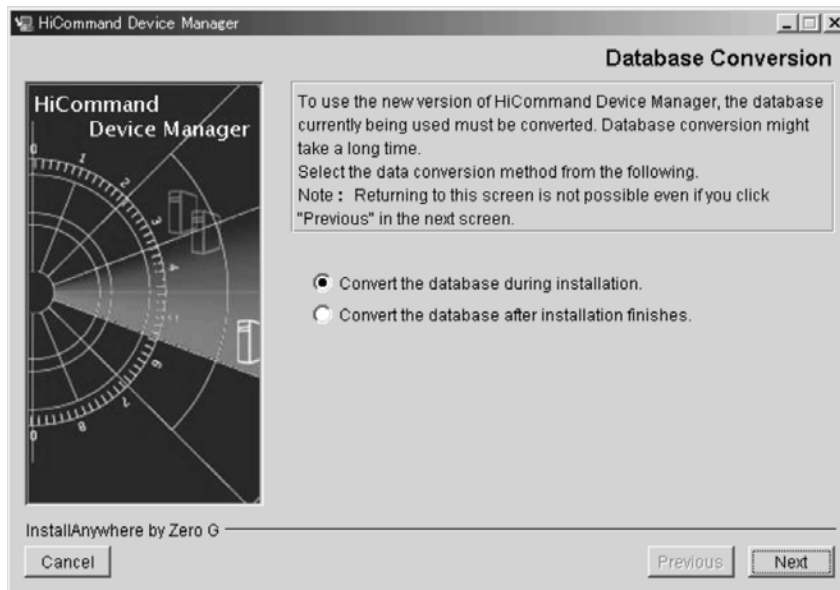


Figure 3.8 Database Conversion Panel

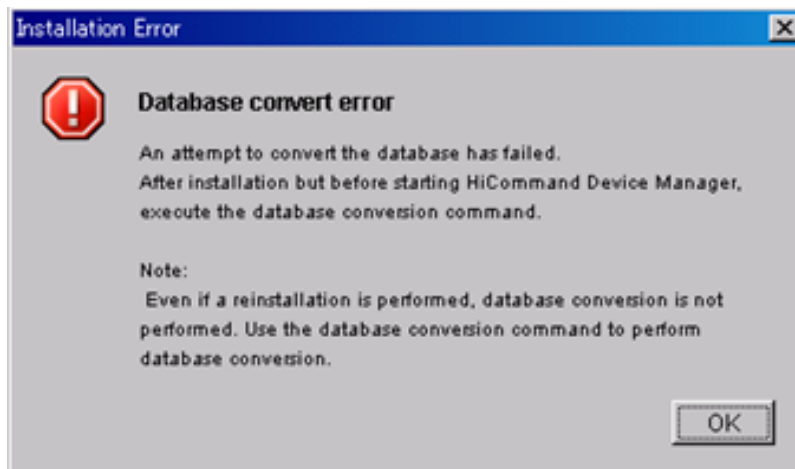


Figure 3.9 Database Convert Error Panel

3.2.3.3 Performing an Upgrade Installation from Version 4.0 or Later or Performing a Re-installation

After finishing an upgrade installation or re-installation, make sure to back up the HiCommand Device Manager server database.

WARNING: Close the Services panel before you perform an upgrade installation or re-installation of the HiCommand Device Manager server. Otherwise, the HiCommand Device Manager server service will be deleted when you close and then re-open the Services panel.

WARNING: Do not cancel in the middle of an upgrade installation or re-installation, as doing so can corrupt the files.

The previous `HiCommandCLI.properties` file is saved as `HiCommandCLI.properties.old` in the same folder. The previous `TIA.properties` file is saved as `TIA.properties.old` in the same folder.

Important: If the `HiCommandCLI.properties` file contains multiple entries of the same key with different values, the value of the most recently specified key overrides the others. Although key duplication does not affect HiCommand CLI operations, we do not recommend that you specify the same key more than once with different values. We recommend that you eliminate unnecessary duplicate keys and their values. If there are duplicate keys that have different values during an upgrade installation, the new `HiCommandCLI.properties` file will inherit keys as follows:

If there are multiple `password` keys:

All `password` keys and their values in the old `HiCommandCLI.properties` file are written to the new file as is. The following shows an example:

- The `password` keys and their values in the old file:
`password=AAA`
`password=BBB`
- The `password` keys and their values written to the new file:
`password=AAA`
`password=BBB`

If there are duplicate keys other than `password`:

The name and value of the most recent duplicate key in the old `HiCommandCLI.properties` file are written to the new file as many times as there are duplicated keys. The following shows an example:

- The `user` keys and their values in the old file:
`user=AAA`
`user=BBB`
- The `user` keys and their values written to the new file:
`user=BBB`
`user=BBB`

Note: Files created by a user will not be saved as `*.old` during the upgrade installation or re-installation.

If you want to manually make a backup before performing an upgrade installation or re-installation of the HiCommand Device Manager server, copy the following files and directories to another location:

- *installation-folder-for-the-Device-Manager-server*\HiCommandServer\config*.properties

The old *.properties files are backed up in the `config` file as `*.properties.old`. Note, however, that files created by a user will not be backed up.

- *installation-folder-for-the-Device-Manager-server*\HiCommandServer\logs

To back up the log files, copy this folder to another location

- *installation-folder-for-the-Device-Manager-server\HiCommandCLI\HiCommandCLI.properties*
The old HiCommandCLI.properties files are backed up as HiCommandCLI.properties.old in the same folder.
- *installation-folder-for-the-Device-Manager-server\HiCommandCLI\legacy\R2.0\HiCommandCLI.properties*
The old HiCommandCLI.properties files are backed up as HiCommandCLI.properties.old in the same folder.
- *installation-folder-for-the-Device-Manager-server\HiCommandCLI\legacy\R2.1\HiCommandCLI.properties*
The old HiCommandCLI.properties files are backed up as HiCommandCLI.properties.old in the same folder.
- *installation-folder-for-the-Device-Manager-server\SupportTools\CollectTool\TIA.properties*
The old TIA.properties files are backed up as TIA.properties.old in the same folder.

Caution: If CIM/WBEM functions are being used when upgrading from version 4.2 or earlier, you must release the registration of the SLP service from the Windows service before performing the upgrade. For details about releasing an SLP service registration, see the *HiCommand Device Manager CIM/WBEM User's Guide*.

If you have performed an upgrade installation without releasing the SLP service registration, it may fail to launch the SLP service after the installation.

In such a case, do the following:

1. Disable the Service Location Protocol service from the **Service** window in Windows.
2. Restart Windows.
3. Release the SLP service registration.
4. Register the SLP service again.

Caution: In version 5.0 or later, user information is managed by using the user management functionality of HiCommand Suite Common Component. The registered user information is migrated to the HiCommand Suite Common Component repository when the Device Manager server program is started for the first time after the upgrade installation. For this migration, also note the following points:

- If there is user information that cannot be migrated to the HiCommand Suite Common Component repository due to data corruption or some other problem, that information is output to the Device Manager trace log file.

- If user accounts with the same user ID but different passwords have been registered in both HiCommand Suite Common Component and Device Manager, the user account in HiCommand Suite Common Component overrides the one in Device Manager. The user account registered in Device Manager becomes unavailable, and information to that effect is output to the Device Manager trace log file. For details about the Device Manager trace log file, see section 5.3.1.
- If user accounts that have the same user ID and password have been registered in both HiCommand Suite Common Component and Device Manager, the user account in Device Manager is added to the one in HiCommand Suite Common Component.
- You cannot migrate the user account whose user ID is `System`. The user management functionality of HiCommand Suite Common Component defines this user ID as having the `Admin` permission for all HiCommand Suite products (version 5.0 or later).

The database can automatically be backed up or exported during installation. If you want to manually back up or export the database, perform the operations specified in sections 3.7.1 or 3.7.3.4. Decide whether to back up or export the database by referring to the following points.

- If version 5.1 or earlier of a HiCommand Suite product is already installed, back up the database. You cannot export the database.
- If version 5.5 or later of a HiCommand Suite product has already been installed and you will perform an upgrade installation, we recommend you export the database.
- If you will perform a re-installation, we recommend you back up the database.

To perform an upgrade installation or re-installation of the HiCommand Device Manager server:

1. Log on to the system as an administrator.
2. Stop any other HiCommand Suite software that is running.
3. Load the Device Manager Server Installation CD. From the **Start** menu, select **Run**, and then **Browse**. Navigate to the CD folder and select **install.exe** from the list of root files.

WARNING: If you attempt to downgrade HiCommand Device Manager, the installer displays the HiCommand Device Manager Upgrade Error panel and exits. However, if the version and revision numbers of the builds before and after a downgrade are the same, the installer displays the WARNING: HiCommand Device Manager Downgrade panel. If there is no problem, select **Next** to continue.

When the HiCommand Suite Common Component services are running, the **Stop HiCommand Suite Common Component Services** panel is displayed. Select **Next** to continue.

If the installer cannot stop the HiCommand Suite Common Component services, the **HiCommand Suite product is running** panel is displayed, and the installation stops. Stop the HiCommand Suite Common Component services manually, and then perform the installation again.

4. The **HiCommand Device Manager Already Installed** panel is displayed.

Note: If the **HiCommand Suite is Running** panel is displayed, you must stop all of the HiCommand Suite Software and then re-start the installation procedure.

5. The **Do you want to back up the database?** panel (see Figure 3.10) or the **Do you want to export the database?** panel (see Figure 3.11) is displayed. After you select whether to back up or export the database as described below, select **Next** to continue. The backup or export will be started based on the options you selected.
 - If you want to back up the database, select **YES. Back up the database during installation.** If you do not want to, select **NO. Do not back up or export the database during installation.**
 - If you want to export the database, select **YES. Export the database during installation.** If you do not want to, select **NO. Do not export the database during installation.**

This operation backs up or exports all HiCommand Suite product databases. The following table describes the conditions whether the backup or export is performed, the backup-data storage destination folder, and the disk space required for the folder.

Table 3.5 Storage Destination of Backed up and Exported Data and Required Disk Space

Operation	Performing conditions	Data storage destination folder	Required disk space
Backup	▪ When the version of HiCommand Suite Common Component is 5.1 or earlier ▪ When the version of HiCommand Suite Common Component is 5.5 or later, and performing a re-installation of the same version and revision of HiCommand Device Manager	<i>HiCommand-installation-folder\olddbbackup_hdb</i>	See section 3.7.1.
Export	When the conditions for backing up data are not satisfied	<i>HiCommand-installation-folder\olddbexported_hdb</i>	See section 3.7.3.4.

Note: Before backing up or exporting, the contents of the data storage destination folder are deleted. Before deletion, a deletion confirmation panel is displayed. If you want to save the old data, you need to copy it to another location beforehand, and then click the **OK** button in the deletion confirmation panel.

Note: Backing up or exporting can fail due to insufficient disk space, or for other reasons. If this occurs, back up or export the databases manually. Then, select **NO. Do not back up the database during installation** for backing up, or select **NO. Do not export the database during installation** for exporting, to continue the installation. For information on how to export a database, see section 3.7.3

Note: The **Do you want to back up the database?** panel or the **Do you want to export the database?** panel is skipped when you return from the next panel after performing backup or export operations.

6. If the Windows Firewall function is installed on the system, the Adding to the Windows Firewall exceptions panel is displayed. Check the contents of the panel, and select **Next** to continue.
7. The **Pre-installation Summary** panel displays. The product name, installation folder, information on installation disk capacity, the IP address or host name of the server machine, and the port number to be used are displayed. Verify that the information is correct, then select **Install** to begin.
 - If you select **Cancel**, the **Cancellation Warning** panel displays, warning you that if you cancel now installation will not complete.
8. The **Please Wait** panel displays, and setup starts after installation, at which point the **Progress** panel displays.
9. The Service Startup Finished panel is displayed. Select **Next** to continue.
10. The **Secure Socket Certificates Note** panel displays.
11. If you plan to run secure socket communications, note the information in this panel for later use. For more information on configuring secure sockets, see Chapter 7. Select **Next** to continue.
12. The **Install Complete** panel displays.
13. Select **Finish** to complete the installation.

If the system is in a cluster configuration, go to step 20.
14. Stop the Device Manager server and HiCommand Suite Common Component.

Select **Start, Program, HiCommand, Device Manager**, and then **Stop Server with Common Services**.
15. Edit the `pdsys` file and the `def_pdsys` file.

Change the value for the `pdunit` parameter's `-x` option to the loopback address `127.0.0.1`.

The default installation locations of the `pdsys` file and `def_pdsys` file are as follows:

installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\pdsys

installation-folder-for-HiCommand-Suite-Common-Component\database\work\def_pdsys
16. Edit the `pdutys` file and the `def_pdutys` file.

Change the value for the `pd_hostname` parameter or to the loopback address `127.0.0.1`.

If `pd_hostname` does not exist, add the `pd_hostname` parameter to set a loopback address.

The default installation locations of the `pdutys` file and `def_pdutys` file are as follows:

installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\pdutys

installation-folder-for-HiCommand-Suite-Common-Component\database\work\def_pdutsys

17. Edit the `HiRDB.ini` file.

Change the value for the `PDHOST` parameter to the loopback address `127.0.0.1`.

The default installation locations of the `HiRDB.ini` file is as follows:

installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\emb\HiRDB.ini

18. Restart the machine.

19. Execute the following command to make sure that the HiCommand Suite Common Component service is running:

installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdssrv
/status

20. Refresh all the registered subsystems to update the database.

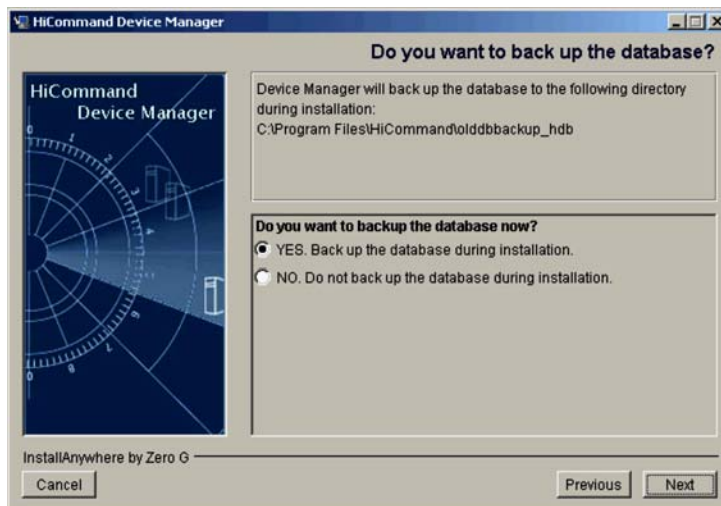


Figure 3.10 Do you want to back up the database? Panel

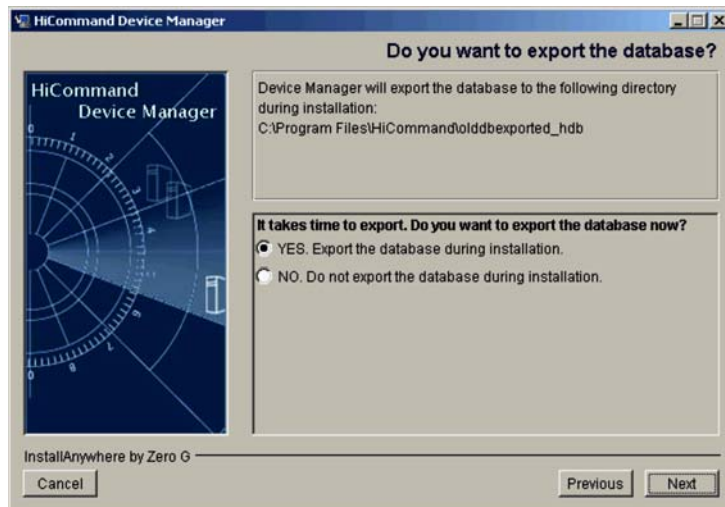


Figure 3.11 Do you want to export the database? Panel

3.3 Installing to a Microsoft Cluster Server Environment

HiCommand Device Manager Server can provide higher availability in a cluster environment. This section discusses the requirements and settings for a cluster environment.

3.3.1 System Requirements for a Cluster Server

The requirements for a cluster environment are as follows:

- Platform: Windows 2000 Advanced Server (SP 4) or Windows Server 2003 Enterprise Edition (without a service pack, or with SP1)
- Cluster software: Microsoft Cluster Service (MSCS)
- Number of nodes: 2
- Cluster configuration: Active-standby configuration

Caution: Disk configuration must be the same on all nodes that make up a cluster, and the installation folder for the Device Manager server must have the same name (including the drive letter and path name).

Caution: During installation, there is a step to back up and migrate the databases. Make sure that you secure the free disk space for backup and migration before installation. For the disk space required to back up, see section 3.7.1. The target disk (that is placed on the shared disk or local disk) to which the database is to be migrated must have the same free disk space or more as the database of the migration source.

3.3.2 Setup Where Other HiCommand Products Are Installed

Follow these instructions when you have other HiCommand Suite products installed in a cluster configuration.

Note: In this procedure, the cluster configuration for other HiCommand Suite products is temporarily cancelled.

Important: When you execute this sequence, it will change the port used by HiRDB to its default (23032). If you are using a port other than the default, you must change it back.

1. Access the Cluster Administrator.
2. For each HiCommand Suite product and the HiRDB service, remove that product from the cluster monitoring target, as follows:
 - Place the target service offline.
 - Right-click each target service, select **Properties**, then select the **Advanced** tab. Select **Do not restart**, and then select **OK**.
3. Stop all HiCommand Suite products in both the executing and standby nodes. See the manuals for the individual products if you need instructions.
4. Stop the Common Component in both the executing and standby nodes:

<common component installation folder>\bin\hcmdssrv /stop

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

5. In the Cluster Administrator, for each group where a HiCommand Suite product service has been registered, switch each group into the standby system by right-clicking a group then selecting **Move Group**.
6. On the standby node, do the following:
 - Start HiRDB:

<common component installation folder>\bin\hcmdsdbsrv /start

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start

- Back up the database (see section 3.7.1 if you need instructions).
- In the standby node, create a database on your local disk.

Delete or empty *target-folder-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdclustersetup  
/removecluster /databasepath target-folder-for-re-creating-the-database /exportpath  
target-folder-for-storing-data
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdclustersetup /removecluster /databasepath  
D:\re_creating_db /exportpath C:\storing_data
```

Caution: Specify an absolute path (maximum of 63 bytes) for *target-folder-for-re-creating-database* and *target-folder-for-storing-data*.

Caution: *target-folder-for-re-creating-database* must be placed on a local disk.

Caution: The characters that can be used for *target-folder-for-re-creating-database* and *target-folder-for-storing-data* are as follows. In addition to these characters, (\), (:), and (/) can be used as path delimiters.

A-Z a-z 0-9 ' ' _

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts HiCommand Suite Common Component.

7. In the Cluster Administrator, switch each group in which the HiCommand Suite product service has been registered into the executing system.

8. On the executing node, do the following:

- Start HiRDB:

<common component installation folder>\bin\hcmdsdbsrv /start

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start

- Back up the database (see section 3.7.1 if you need instructions).
- In the executing node, migrate the database to your local disk.

Delete or empty *target-folder-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

<i>installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup /removecluster /databasepath target-folder-for-re-creating-the-database /exportpath target-folder-for-storing-data</i>
--

The following shows an example of executing the command:

<i>C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /removecluster /databasepath D:\re_creating_db /exportpath C:\storing_data</i>

Caution: Specify an absolute path (maximum of 63 bytes) for *target-folder-for-re-creating-database* and *target-folder-for-storing-data*.

Caution: *target-folder-for-re-creating-database* must be placed on a local disk.

Caution: The characters that can be used for *target-folder-for-re-creating-database* and *target-folder-for-storing-data* are as follows. In addition to these characters, (\), (:), and (/) can be used as path delimiters.

A-Z a-z 0-9 ' ' _

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts HiCommand Suite Common Component.

9. Install HiCommand Device Manager server and configure a cluster environment by referring to section 3.2.2.

For information on how to setup a cluster environment for other HiCommand Suite products, see the relevant manual for each product.

3.3.3 Performing a New Installation

After finishing a new installation, be sure to back up the Device Manager server database.

Caution: While performing cluster configuration, do not access HiCommand Device Manager.

Note: Before installing Device Manager, make sure that the cluster management IP address and shared disk are enabled on the executing node.

3.3.3.1 Installing on the Executing Node

1. If the service of another HiCommand Suite product or cluster group exists, exclude it from cluster management.
2. On the executing node, perform a new installation of the Device Manager server (see section 3.2.2). The following are the requirements for the installation:
 - Leave the settings specifying the location of the Common Component and the Device Manager Server databases at their default values (see Figure 3.2 and Figure 3.3).
 - For the IP address of the Device Manager Server, specify a logical host name (see Figure 3.4).

Important: A logical host name indicates the name of a virtual host allocated to the cluster management IP address.

3. After the Device Manager Server is installed on the executing node, enter the license key by using the Web Client.

Note: You should have received a CD that contains the HiCommand Device Manager License Key. You should upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found simply highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.

4. Use a text editor to create a cluster configuration file, as follows:
 - **mode:** Specify online.
 - **virtualhost:** Specify the logical host name.
 - **onlinehost:** Specify the host name of the executing node.
 - **standbyhost:** Specify the host name of the standby node.

Sample command:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

5. Save the created file as **cluster.conf** in **<common component installation folder>\conf**.

Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

Caution: An IP address that is enabled and accessible must be assigned to the logical host name to be specified in `virtualhost`.

6. Stop the Device Manager Server and HiCommand Suite Common Component by selecting **Start → Programs → HiCommand → Device Manager → Stop Server with Common Services**.

WARNING: Do not use the Windows Services panel to stop the Device Manager Server.

7. Start HiRDB by executing the following command:

<common component installation folder>\bin\hcmsdbserve /start

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmsdbsrv /start

8. Back up the database (see section 3.7.1 if you need instructions).
9. Migrate the database to the shared disk.

Delete or empty *target-folder-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmsdbclustersetup  
/createcluster /databasepath target-folder-for-re-creating-the-database /exportpath  
target-folder-for-storing-data
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmsdbclustersetup /createcluster /databasepath  
R:\re_creating_db /exportpath C:\storing_data
```

Caution: Specify an absolute path (maximum of 63 bytes) for *target-folder-for-re-creating-database* and *target-folder-for-storing-data*.

Caution: *target-folder-for-re-creating-database* must be placed on a shared disk. *target-folder-for-storing-data* must be placed on your local disk.

Caution: The characters that can be used for *target-folder-for-re-creating-database* and *target-folder-for-storing-data* are as follows. In addition to these characters, (\), (:), and (/) can be used as path delimiters.

```
A-Z a-z 0-9 ' ' _
```

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts HiCommand Suite Common Component.

10. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

<common component installation folder>\bin\hcmdssrv /stop

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

11. Open the **Services** panel. For each of the following services, open the property, and then change Startup Type from **Automatic** to **Manual**:

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiCommand Server

3.3.3.2 Installing on Standby Node

The following are the specific requirements for installation on the standby node:

- Specify the same installation path as on the executing node (see Figure 3.1).
- Leave the settings specifying the location of the Common Component and the Device Manager Server databases at the default values (see Figure 3.2 and Figure 3.3).
- For the IP address of the Device Manager Server, specify a logical host name (see Figure 3.4).

1. On the standby node, perform a new installation of the Device Manager Server. When the Back up the database panel displays (see Figure 3.10), select **NO. Do not back up or export the database during installation.**

Important: A logical host name indicates the name of a virtual host allocated to the cluster management IP address.

2. After the Device Manager Server is installed on the standby node, enter the license key by using the Web Client. For more information on using the Web Client, please see the *HiCommand Device Manager Web Client User's Guide*.

Note: You should have received a CD that contains the HiCommand Device Manager License Key. You should upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found simply highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.

3. Use the IP address of the standby node to access the Device Manager Server.
4. Use a text editor to create a cluster configuration file. The items to be specified in the cluster configuration file are as follows:
 - **mode:** Specify standby.
 - **virtualhost:** Specify the logical host name.
 - **onlinehost:** Specify the host name of the executing node.
 - **standbyhost:** Specify the host name of the standby node.

Sample command:

```
mode = standby
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

5. Save the created file as cluster.conf in **<common component installation folder>\conf**.

Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

6. Stop the Device Manager Server and Common Component as follows:

Select **Start → Programs → HiCommand → Device Manager → Stop Server with Common Services**

WARNING: Do not use the **Services** panel to stop the Device Manager Server.

7. Change the setting so that the database on the shared disk is to be used:

When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

<common component installation folder>\bin\hcmdsdbremake /cluster /databasepath <database target folder>

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdsdbremake /cluster /databasepath R:\re_creating_db

Caution: Specify the same folder as the folder specified for <database target folder> on the executing node. Do not use a path delimiter at the end of the folder name.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts the Common Component.

8. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

<common component installation folder>\bin\hcmdssrv /stop

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

9. Open the **Services** panel. For each of the following services, open the property, and then change Startup Type from **Automatic** to **Manual**:
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiCommand Server

3.3.3.3 Configuring Microsoft Cluster Server During a New Installation

1. Open the Cluster Administrator:

Select **Start, Settings, Control Panel, Administrative Tools**, and then **Cluster Administrator**.
2. If there is an existing group in which to register the Device Manager service, select that group. If there is not, create one.

Caution: Use only resources related to HiCommand Suite products to configure the resource group.

3. Select **IP address** in **Resource type** to register the cluster management IP address to a resource group.
4. Select **Network name** in **Resource type** to register the logical host name to a resource group.
5. Select **Physical disk** in **Resource type** to register the shared disk to a resource group.
6. Register HBase Storage Mgmt Common Service, HBase Storage Mgmt Web Service, HiCommandServer, and HiRDB as resources. Select **New**, and then **Resource**. In each panel, specify the settings as shown in the following tables.

Table 3.6 Settings to Register HiRDB as a Resource

Dialog box Name	Setting
New Resource	Name: HiRDB (optional) Resource type: Generic Service.
Possible Owners	Make sure that the executing and standby nodes have been added.
Dependencies	Register the drive of the shared disk drive and network name.
Generic Service Parameters	Service Name: HiRDBClusterService_HD0 Start parameters: None
Registry Replication	Specify nothing.

Table 3.7 Settings to Register the HBase Storage Mgmt Common Service as a Resource

Dialog box Name	Setting
New Resource	Name: Mgmt Common Service (optional) Resource type: Generic Service.
Possible Owners	Make sure that the executing and standby nodes have been added.
Dependencies	Register HiRDB.
Generic Service Parameters	Service Name: HBaseStgMgmtComService Start parameters: None
Registry Replication	Specify nothing.

Table 3.8 Settings to Register the HBase Storage Mgmt Web Service as a Resource

Dialog box Name	Setting
New Resource	Name: Mgmt Web Service (optional) Resource type: Generic Service.
Possible Owners	Make sure that the executing and standby nodes have been added.
Dependencies	Register Mgmt Common Service.
Generic Service Parameters	Service Name: HBaseStgMgmtWebService

	Start parameters: None
Registry Replication	Specify nothing.

Table 3.9 Settings to Register the HiCommand Device Manager Server as a Resource

Dialog box Name	Setting
New Resource	Name: HiCommandServer (optional) Resource type: Generic Service.
Possible Owners	Make sure that the executing and standby nodes have been added.
Dependencies	Register the Mgmt Web Service.
Generic Service Parameters	Service Name: HiCommandServer Start parameters: None
Registry Replication	Specify nothing.

7. In Cluster Administrator, place the group to which the HiCommand Device Manager service has been registered online.

3.3.4 Performing an Upgrade Installation from Version 3.5 or Earlier

After finishing an upgrade installation, be sure to back up the HiCommand Device Manager server database.

WARNING: If you have made any changes to **<common component installation folder>\conf\init.conf**, and you are upgrading from Device Manager version 4.0 or 4.1 to version 4.2 or later.

3.3.4.1 Upgrading Device Manager on the Executing Node

1. Display the cluster administrator:

Start → Settings Control Panel Programs → Administrative Tools → Cluster Administrator

Note: When the Device Manager Server is upgraded from version 3.5 or earlier to 4.0 or later, these menu options are deleted.

2. Place the following services offline:

- HiCommand Server
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service

The above services are represented by the resource names registered in section 3.3.3.3.

3. For each of those services, in the Cluster Administrator, right-click the service, select **Properties**, select the **Advanced** tab, select **Do not restart**, and then select **OK**.
4. Back up the databases (see section 3.7.1).

5. When you perform the upgrade installation, be sure to specify the local disk as the location of the Common Component and HiCommand Device Manager Server databases (see Figure 3.2 and Figure 3.3), and perform database conversion during the installation (see Figure 3.8).
6. Use a text editor to create a cluster configuration file, as follows:
 - **mode:** Specify `online`.
 - **virtualhost:** Specify the logical host name.
 - **onlinehost:** Specify the host name of the executing node.
 - **standbyhost:** Specify the host name of the standby node.

Sample command:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

7. Save the created file as `cluster.conf` in **<common component installation folder>\conf**.
8. **Caution:** You cannot specify an IP address for `virtualhost`, `onlinehost`, or `standbyhost`. Confirm that the IP address can be resolved from the host name.
9. Stop the Device Manager Server and Common Component as follows:
 Select **Start → Programs → HiCommand → Device Manager → Stop Server with Common Services**
WARNING: Do not use the **Services** panel to stop the Device Manager Server.
10. Start HiRD8 by executing the following command:
<common component installation folder>\bin\hcmdsdbsrv /start
 The following shows an example of executing the command:
C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
11. Back up the database (see section 3.7.1 for instructions).
12. Migrate the database to the shared disk.

Delete or empty *target-folder-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup /createcluster /databasepath target-folder-for-re-creating-the-database /exportpath target-folder-for-storing-data
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster /databasepath R:\re_creating_db /exportpath C:\storing_data
```

Caution: Specify an absolute path (maximum of 63 bytes) for *target-folder-for-re-creating-database* and *target-folder-for-storing-data*.

Caution: *target-folder-for-re-creating-database* must be placed on a shared disk. *target-folder-for-storing-data* must be placed on your local disk.

Caution: The characters that can be used for *target-folder-for-re-creating-database* and *target-folder-for-storing-data* are as follows. In addition to these characters, (\), (:), and (/) can be used as path delimiters.

A-Z	a-z	0-9	'	'	'_'
-----	-----	-----	---	---	-----

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

13. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

<common component installation folder>\bin\hcmdssrv /stop

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

14. Open the **Services** panel. Open the property for the following services, and then change **Startup Type** from **Automatic** to **Manual**:
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiCommand Server

3.3.4.2 Upgrading Device Manager on the Standby Node

1. Open the **Services** panel. Start the following services:
 - InterBase
 - InterBase Server
2. Access **<server installation folder>\HiCommandServer\database\interbase.**
3. Change the file name of the **HICOMMAND.GDB_org** file to **HICOMMAND.GDB.**
4. Change the file name of the **HiCommand.gbk_org** file to **HiCommand.gbk.**
5. Use a text editor to open the following property file:

<server installation folder>\HiCommandServer\config\database.properties
6. Change the line beginning with **dbm.url=** as shown below:

dbm.url=jdbc:interbase://localhost/<server installation folder>\HiCommandServer\database\interbase\HICOMMAND.GDB

Caution: Use a forward slash (/), not a backslash (\) for the path delimiter.
7. Access **<common component installation folder>\database.**
8. Change the file name of the **HBASE.GDB_org** file to **HBASE.GDB.**
9. Use a text editor to open the following file:

<common component installation folder>\conf\user.conf

10. If this file does not already exist, create the file.

11. Change the line beginning with DATABASE.path= as shown below:

DATABASE.path= <common component installation folder>/database/HBASE.GDB

If this line does not already exist, create the line.

Caution: Use a forward slash (/), not a backslash (\) for the path delimiter.

12. On the standby node, perform an upgrade installation of the Device Manager Server.
Make sure of the following:

Leave the settings specifying the location of the Common Component and the Device Manager Server as the default values (see Figure 3.2 and Figure 3.3).

If you are upgrading from version 4.0 or higher, do not convert the database (see Figure 3.8).

13. Use a text editor to create a cluster configuration file.

14. The items to be specified in the cluster configuration file are as follows:

- **virtualhost:** Specify the logical host name.
- **onlinehost:** Specify the host name of the executing node.
- **standbyhost:** Specify the host name of the standby node.

Sample command:

```
mode = standby
virtualhost = hcmsdserver
onlinehost = hcmsdserver_1
standbyhost = hcmsdserver_2
```

15. Save the created file as cluster.conf in **<common component installation folder>\conf**.

Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

16. Stop the Device Manager Server and Common Component as follows:

Select **Start → Programs → HiCommand → Device Manager → Stop Server with Common Services**.

WARNING: Do not use the Windows Services panel to stop the Device Manager Server.

17. Change the setting so that the database on the shared disk is to be used:

When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

<common component installation folder>\bin\hcmsdsqlmake /cluster /databasepath <database target folder>

The following shows an example of executing the command:

**C:\Program Files\HiCommand\Base\bin\hcmsdsqlmake /cluster /databasepath
R:\re_creating_db**

Caution: Specify the same folder as the folder specified for <database target folder> on the executing node.

Caution: Do not specify a path delimiter (\) in <database target folder>, or you will cause an error.

Important: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts the Common Component.

18. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

<common component installation folder>\bin\hcmdssrv /stop

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

19. In the **Services** panel, open the properties for the following services, and then change Startup Type from Automatic to Manual:
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiCommand Server

3.3.4.3 Configuring Microsoft Cluster Server During an Upgrade Installation

1. Display the Cluster Administrator:

Start → Settings Control Panel Programs → Administrative Tools → Cluster Administrator

Note: When the Device Manager Server is upgraded from version 3.5 or earlier to 4.0 or later, these menu options are deleted.

2. Specify the following services in the cluster resources. Make the same settings for each parameter of the resources as in a new installation:
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - HiCommand Server
 - HiRDB
3. If no other resources are depending on InterBase and InterBase Server, you can delete them.
4. In Cluster Administrator, right-click the following services, select **Properties**, select the **Advanced** tab, select **Restart**, and then select **OK**:
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiCommand Server

The above services are represented by the resource names registered in step 2.

5. In Cluster Administrator, place the group to which the Device Manager service has been registered online.

3.3.4.4 Performing an Upgrade or Re-installation of Device Manager on the Executing Node

This section describes how to perform an upgrade installation of HiCommand Device Manager from version 4.0 or later and how to re-install the same version of HiCommand Device Manager by overwriting in a cluster environment.

Warning: After finishing an upgrade installation or re-installation, make sure to back up the HiCommand Device Manager server database.

Caution: If the service is not online on the executing node, first place it online, and then perform an upgrade installation or re-installation.

1. Display Cluster Administrator:

Select **Start, Settings, Control Panel, Administrative Tools**, and then **Cluster Administrator**.

2. Place the following services offline:

- HiCommand Server
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service

The above services are represented by the resource names registered in section 3.3.3.3.

3. Stop the Common Component:

<common component installation folder>\bin\hcmdssrv /stop

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

4. In Cluster Administrator, place the **HiRDB** service offline.

The above service is represented by the resource name registered in section 3.3.3.3.

5. In Cluster Administrator, right-click the following services, select **Properties**, select the **Advanced** tab, **Do not restart**, and then **OK**:

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiCommand Server
- HiRDB

The above services are represented by the resource names registered in section 3.3.3.3.

6. Perform an upgrade installation or re-installation of the HiCommand Device Manager server (see section 3.2.3.3). When the **Do you want to back up the database?** panel is displayed, choose **YES. Back up the database during installation** (see Figure 3.10). When the **Do you want to export the database?** panel is displayed, choose **YES. Export the database during installation** (see Figure 3.11).
7. Stop the HiCommand Device Manager service and the Common Component as follows:
Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server with Common Services**.
8. In the **Services** panel, open the properties for the following services, and then change **Startup Type** from **Automatic** to **Manual**:
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiCommand Server
9. Place the group to which the HiCommand Device Manager service has been registered on standby. In Cluster Administrator, right-click the group to which the HiCommand Device Manager service has been registered, and then choose **Move Group**.

3.3.4.5 Performing an Upgrade or Re-installation of Device Manager on the Standby Node

1. Perform an upgrade installation or re-installation of the HiCommand Device Manager server (see section 3.2.3.3). Do NOT back up the database during installation.
Caution: Even when the **Do you want to back up the database?** panel or the **Do you want to export the database?** panel is displayed, do not perform either operation. If you perform the backup or export operation, installation will fail (see Figure 3.10 and Figure 3.11).
2. Stop the HiCommand Device Manager service and Common Component as follows:
Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server with Common Services**.
3. In the **Services** panel, open the property for the following services, and then change Startup Type from **Automatic** to **Manual**:
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiCommand Server
4. In Cluster Administrator, right-click the following services, select **Properties**, select the **Advanced** tab, select **Restart**, and then select **OK**:
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HiCommand Server
 - HiRDB

The above services are represented by the resource names registered in section 3.3.3.3.

5. In Cluster Administrator, place the group to which the HiCommand Device Manager service has been registered online.

3.3.5 Changing to a Cluster Environment after Starting HiCommand Device Manager Server

When you want to change to a cluster configuration after the HiCommand Device Manager system operations have started in a non-cluster configuration, carry out the following procedure. In this example, the HiCommand Device Manager server whose operations are already running is treated as an executing node.

1. Install the HiCommand Device Manager server on the host to be used as a standby node.
2. On the standby node, display the Web Client login window and then enter the license key.
3. On the executing and standby nodes, stop the HiCommand Device Manager server and HiCommand Suite Common Component as follows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server with Common Services**.

4. On the executing node, start HiRDB.

Execute the following command:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdsrv /start
```

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdsdsrv /start

5. On the executing node and standby node, use the text editor to create a cluster-configuration file for each node.

The items to be specified in the cluster-configuration file are as follows:

mode: Specify *online* for the executing node, and *standby* for the standby node.

virtualhost: Specify the logical host name.

onlinehost: Specify the host name of the executing node.

standbyhost: Specify the host name of the standby node.

The following shows a coding example in the cluster-configuration file on the executing node:

```
mode = online
virtualhost = hcmsdserver
onlinehost = hcmsdserver_1
standbyhost = hcmsdserver_2
```

Save the created file as *cluster.conf* in *installation-folder-for-HiCommand-Suite-Common-Component\conf*.

Caution: An IP address cannot be specified for *virtualhost*, *onlinehost*, or *standbyhost*. Make sure that the IP address can be resolved from the host name.

Caution: An IP address that is enabled and accessible must be assigned to the logical host name to be specified in *virtualhost*.

6. Back up the database (see section 3.6.2).

7. In the executing node, migrate the database to shared disk.

Delete or empty *target-folder-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup  
/createcluster /databasepath target-folder-for-re-creating-the-database /exportpath  
target-folder-for-storing-data
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster /databasepath  
R:\re_creating_db /exportpath C:\storing_data
```

Execute the following command:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbmove /import  
/datapath target-folder-for-storing-data
```

Caution: Specify an absolute path (maximum of 63 bytes) for *target-folder-for-re-creating-database* and *target-folder-for-storing-data*.

Caution: *target-folder-for-re-creating-database* must be placed on a shared disk. *target-folder-for-storing-data* must be placed on your local disk.

Caution: The characters that can be used for *target-folder-for-re-creating-database* and *target-folder-for-storing-data* are as follows. In addition to these characters, (\), (:), and (/) can be used as path delimiters.

```
A-Z a-z 0-9 ' ' ' _
```

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

8. On the standby node, change the setting so that the database on the shared disk is to be used.

Execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbremake /cluster  
/databasepath target-folder-for-re-creating-database
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbremake /cluster /databasepath  
R:\re_creating_db
```

Caution: Specify the same folder as the folder specified for *target-folder-for-re-creating-database* on the executing node.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts HiCommand Suite Common Component on the standby node.

9. If HiCommand(R) Suite Common Component is running on both the executing and standby nodes, execute the following command to stop it.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdssrv /stop
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
```

10. In both the executing node and standby node, change the settings so that the following services start manually.

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiCommandServer

In the Services panel, open the properties of each service, and then change **Automatic** to **Manual** in **Startup Type**.

11. Register (in the cluster software) the resource.

For details on how to register a cluster resource, see section 3.3.3.3.

3.4 Converting the Database

3.4.1 Manually Converting from InterBase to HiRDB

If you have a Device Manager database for versions 2.3 through 3.5, it is based on InterBase. Databases for versions 4.0 and higher are based on HiRDB, so if you are upgrading to that level you will need to convert the database.

Caution: InterBase, InterServer, and HiRDB must all be running when you convert the database.

Note: Database conversion can be a lengthy process. For example, if 8,000 LDEVs and 16,000 paths have been managed, the database conversion will take about 5 minutes in an environment that has a 1.5 GHz CPU and 1 GB of memory. See the Release Notes for more information.

You can either convert the database automatically when you install the Device Manager Server, or manually after the installation using the following procedure.

To manually convert a database:

1. Stop the Device Manager Server:

Select **Start → Programs → HiCommand → Device Manager → Stop Server with Common Services**.

2. Access the **Services** panel, and verify that the following services are running:

- InterBase Server
- InterServer

3. Verify that HiRDB is running:

<common component installation folder>\bin\hcmdssrv /status

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /status

4. The following message should display:

KAPM06440-I The HiRDB service has already started.

5. If HiRDB is not running, start it by executing the following command:

<common component installation folder>\bin\hcmdssrv /start

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /start

6. From the command prompt, execute the **migrateFmIB** command.

The default installation folder for the migrateFmIB command is as follows:

<server installation folder>\migrateFmIB.bat

The command format is as follows:

migrateFmIB [-d InterBase-GDB-file-name | InterBase-GBK-file-name] [-u InterBase-user-id] [-p InterBase-password]

The following shows an example of executing the command:

**C:\Program Files\HiCommand\DeviceManager\migrateFmIB -d C:\IBdata\ibase.gdb
-u ibuser1 -p sys0305**

The following options can be specified for the migrateFmIB command:

-d: Specify an absolute path for the name of the GDB or GBK file for InterBase. If this option is not specified, the following file is used

<Device Manager Server installation folder>\HiCommandServer\database\interbase\HiCommand.gdb

-u: Specify the InterBase user ID. The default InterBase user ID is assumed if the -u option is not specified.

-p: Specify the InterBase password. The password of the default InterBase user ID is used if the -p option is not specified.

7. Specify **true** for the **server.base.initialsynchro** property in the server.properties file. See section 8.2.23 for more information.
8. Restart the Device Manager Server:
Select **Start → Programs → HiCommand → Device Manager → Start Server**
9. In the server.properties file, change the **server.base.initialsynchro** property back to false. The results are returned as a return code (see Table 3.10).

Table 3.10 Return Codes for migrateFmIB Command

Return code	Description
0	The command terminated normally.
1	InterBase is not running.
2	HiRDB is not running.
3	An InterBase authentication error occurred.
4	A HiRDB authentication error occurred.
5 to 19	(Reserved)

20	The HiCommand Device Manager Server is running.
21 to 29	(Reserved)
30	The database file to be converted does not exist.
31 to 39	(Reserved)
40	An attempt to change the database definition has failed.
41 to 49	(Reserved)
50	An attempt to convert the database has failed.
51 to 253	(Reserved)
254	An error occurred during conversion processing.
255	Internal error

3.4.2 Converting to a Cluster Configuration

This section contains instructions for changing to a cluster configuration after you have already started operating under a non-cluster configuration. In this example, the Device Manager Server where operations are already running is treated as the executing node.

1. On the host that will be used as the standby node, install the Device Manager Server. See section 3.3 if you need instructions.
2. On the standby node, display the Web Client logon window, then enter the license key.

Note: Your product installation CD should contain the HiCommand Device Manager License Key. If you upload the License Key file to a directory on the same server where Device Manager will be installed, you can select the button next to **License File** and browse for the License Key file. Once the file is found, simply highlight the file and select the **Open** button. This updates Device Manager with the permanent License Key.

3. On the executing and standby nodes, stop the Device Manager service and Common Component as follows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server with Common Services**.

4. On the executing node, start HiRDB by executing the following command:
<common component installation folder>\bin\hcmdsdbsrv /start
5. On the executing node, delete or empty the **<database target folder>**, then back up the database contents:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbmove /export
/datapath target-folder-for-storing-data
```

Caution: Before executing the command, delete or empty the *target-folder-for-storing-data*.

Caution: Specify an absolute path for the *target-folder-for-storing-data*.

6. On both the executing and standby nodes, use a text editor to create a cluster configuration file for each node. Specify the following:
 - **mode:** Specify **online** for the executing node, and **standby** for the standby node

- **virtualhost:** Specify the logical host name
- **onlinehost:** Specify the host name of the executing node
- **standbyhost:** Specify the host name of the standby node

Sample command:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

7. Save the created file as **cluster.conf** in **<common component installation folder>\Conf**.

Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

8. Re-create the database system on the shared disk of the executing node:

<common component installation folder>\bin\hcmdsdbremake /cluster /databasepath <database target folder>

Caution: The file name for <database target folder> must be no more than 63 bytes, and you must specify an absolute path to it.

Caution: On the shared disk, deploy the folder in which the database is to be re-created.

Caution: When this command is executed, the port designated for HiRDB to use returns to the default (23032). If you use another port for HiRDB, you must reset the port after this operation.

Important: You must specify an absolute path to the target directory. Do not use a path delimiter (\) at the end of the target directory name, or you will get a command error. If this occurs, remove the path delimiter and re-execute the command.

Note: This operation restarts the Common Component on the executing node.

9. Back up the database (see section 3.7.1 for instructions).
10. Register the database contents that were backed up in step 5:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbmove /import
/datapath target-folder-for-storing-data
```

Caution: : Specify an absolute path for the *target-folder-for-storing-data*.

11. On the standby node, change the setting so that the database on the shared disk is to be used:

<common component installation folder>\bin\hcmdsdbremake /cluster /databasepath <database target folder>

Caution: Specify the same folder as the folder specified for <database target folder> on the executing node.

Caution: When this command is executed, the port designated for HiRDB to use returns to the default (23032). If you use another port for HiRDB, you must reset the port after this operation.

Important: You must specify an absolute path to the target directory. Do not use a path delimiter (\) at the end of the target directory name, or you will get a command error. If this occurs, remove the path delimiter and re-execute the command.

Note: This operation restarts the Common Component on the standby node.

12. Stop the Common Component in both the executing and standby nodes:

<common component installation folder>\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

13. In both the executing node and standby node, change the settings so that HiCommand Server starts manually.

14. In the **Services** panel, open the properties of HiCommand Server, and then in Startup Type change **Automatic** to **Manual**.

15. Register the resource in the cluster software.

3.5 Verifying Installation of Device Manager Server and Common Component

After you complete the installation, you need to verify that the following services are either running or can be started manually:

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- Device Manager Server

If all of these services can be started, the installation was successful. If one or more of these services either does not appear in the **Services** panel or cannot be started, the installation has failed.

1. Enter the following command to verify that the Common Component is installed:

<installation folder>\Base\sample\conf\build

2. If the Common Component is installed, you will see a six-digit build number (for example, 030501) in the file.

Caution: Even if installation of HiCommand Device Manager fails, the **GO** menu command for starting HiCommand Device Manager might appear in the Dashboard of other HiCommand Suite products. To remove **GO**, a user with User Management permissions must execute the following command. When this command is executed, the HiCommand Suite Common Component services must be running.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsintg /delete /type  
DeviceManager /user user-ID /pass password
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsintg /delete /type DeviceManager /user dvmuser1  
/pass sys0305
```

3.5.1 HBase Storage Mgmt Common Service or HBase Storage Mgmt Web Service Fails to Start

If the HBase Storage Management Common or Web Service fails to start, possible problems and solutions include the following:

- The port number might already be in use. If this is the case, change the port number. See section 8.2 for instructions on how to change the port.
- The amount of installed memory might be insufficient. To increase the amount of installed memory as needed, see section 3.1.1.

Caution: Even after attempting to fix the problem, if the HBase Storage Mgmt Common Service and HBase Storage Mgmt Web Service still do not start, restart the Device Manager server.

Caution: If the cause of the problem is uncertain, and the HBase Storage Mgmt Common Service or Web Service still fail to start, use the **hcmdsgetlogs** command to collect maintenance information, and then contact Customer Support. For more information on the **hcmdsgetlogs** command, see section 10.2.1.

3.5.2 HBase Storage Mgmt Common or Web Service Does Not Appear in Services

If either the HBase Storage Mgmt Common Service or the HBase Storage Mgmt Web Service is not displayed in the **Services** panel, installation of the Common Component may have failed.

Check the install log, which is in the installation directory. If you find the error, follow the instructions in the error message.

If problems still exist, uninstall Device Manager (see section 3.8.1 for instructions), reboot the system, and re-install Device Manager (see section 3.2.2 for instructions).

3.5.3 Device Manager Server Fails to Start

If the Device Manager Server fails to start, the installation may have failed. Examine the trace log at **installation-folder-for-the-Device-Manager-server\HiCommandServer\log\HDvMtrace*.log**, review the error codes, and follow the recommended actions. For more information about error codes, see *HiCommand Device Manager Error Codes* (MK-92HC016).

3.5.4 HiCommand Device Manager Server Does Not Appear in the Services Panel

If the Device Manager Server does not appear in the **Services** panel, the installation may have failed.

The basic troubleshooting procedure in the event of installation failure or other problems is to uninstall Device Manager (see 3.8.2 for instructions), and reboot the system. Verify that all of the requirements have been met (see section 3.1), then re-install Device Manager (see section 3.2 for instructions).

3.6 Starting and Stopping Device Manager Server

WARNING: If a Device Manager client (e.g., Web Client, Device Manager CLI, or Device Manager Agent) is accessing the Device Manager Server when that machine is shut down, the Device Manager client processing will terminate. Make sure that Device Manager clients are not accessing the server before shutting down a machine that is running the Device Manager Server.

Note: Device Manager server 5.0 or later can start and stop independently. It can also start or stop HiCommand Suite Common Component synchronously. In addition, a synchronized Device Manager server and HiCommand Suite Common Component can be restarted automatically after they are stopped.

3.6.1 Starting and Stopping Using Windows Functions

This section describes how to start or stop the HiCommand Device Manager server and HiCommand Suite Common Component from the **Start** menu.

- To start the HiCommand Device Manager server:
Select **Start → Programs → HiCommand → Device Manager → Start Server**
- Starting the HiCommand Device Manager Server and Common Component:
Select **Start → Programs → HiCommand → Device Manager → Start Server with Common Services**
- Restarting the HiCommand Device Manager Server and Common Component:
Select **Start → Programs → HiCommand → Device Manager → Restart Server with Common Services**

To check status, use one of the following sequences:

- **Start → Programs → HiCommand → Device Manager → Server Status**
- **Start → Programs → HiCommand → Device Manager → Server and Common Services Status**

Stop the Device Manager Server alone or together with the Common Component by using one of the following sequences:

- **Start → Programs → HiCommand → Device Manager → Stop Server**
- **Start → Programs → HiCommand → Device Manager → Stop Server with Common Services**

3.6.2 Starting and Stopping Using Device Manager Commands

This section describes how to start or stop the HiCommand Device Manager server and HiCommand Suite Common Component by using commands.

To start the Device Manager Server, execute the following command:

<Device Manager Server installation folder>\suitesrvctl /start_hdvm

The following shows an example of executing the command:

C:\Program Files\HiCommand\DeviceManager\suitesrvctl /start_hdvm

This command outputs the following messages:

```
The HiCommandServer service is starting.  
The HiCommand Server service was started successfully.
```

To stop the Device Manager Server, execute the following command:

<Device Manager Server installation folder>\suitesrvctl /stop_hdvm

To check the status of the Device Manager Server, execute the following command:

<Device Manager Server installation folder>\suitesrvctl /status_hdvm

Note: *status2* is an interface used by other applications to check the status of the HiCommand Device Manager Server. If you replace the command parameter *status* with *status2*, a return code (see Table 3.11) is displayed.

Table 3.11 status2 Return Codes

Return Code	Description
0	Startup operations for the Device Manager Server have finished.
1	Device Manager Server is not running.
2	Device Manager Server is running.
3~99	Other status.
100	The server.properties file was not found.
101~199	External error.
200	The value of server.http.port in the server.properties file is invalid.
201~999	External error.
1000~65535	Internal error.

- To start the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

<Device Manager Server installation folder>\suitesrvctl /start_all

- To stop the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

<Device Manager Server installation folder>\suitesrvctl /stop_all

- To restart the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

<Device Manager Server installation folder>\suitesrvctl /restart_all

- To check the status of the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

<Device Manager Server installation folder>\suitesrvctl /status_all

Caution: Do not execute the `hcmdssrv`, `hdvmsrvctl`, or `suitesrvctl` command while the `suitesrvctl` command is being executed. If you do so, the `suitesrvctl` command may not operate correctly. If you have done so inadvertently, re-execute the `suitesrvctl` command. Also, do not execute the `suitesrvctl` command while the `hicommand` or `hcmdssrv` command is being executed.

3.7 Operating the HiCommand Device Manager Server Database

This section describes how to perform the following operations for the Device Manager server database:

- Backing up
- Restoring the backed-up data
- Migrating the database (export and import)
- Initializing the database

The following table shows the differences in the functions between backing up and restoring verses exporting and importing.

Table 3.12 Backing Up and Restoring Verses Exporting and Importing

Item	Backing up and restoring	Exporting and importing
Conditions of the HiCommand Suite Common Component version	No limitation.	HiCommand Suite Common Component version 5.5 or later must be installed on the machine used for the export source or the import destination.
Main purpose of use	To recover the current operating environment when a failure occurs in the server machine.	To migrate the server machine from the current environment to a different environment (such as a machine with a different OS).
Target data	■ Databases for HiCommand Suite products ■ The HiCommand Suite Common Component database	■ Databases for HiCommand Suite products ■ User information included in the HiCommand Suite Common Component database
Conditions for the machine used for the restore destination or the import destination	The following must be the same in the backup source machine and the restore destination machine: ■ Types, versions, and revisions of the installed HiCommand Suite products ■ Installation locations for each HiCommand Suite product, HiCommand Suite Common Component, each HiCommand Suite product database, and HiCommand Suite Common Component database	■ The HiCommand Suite products whose databases to be imported must be installed. ■ The versions of the installed HiCommand Suite products must be the same as or higher than the ones on the export source machine.

	▪ The IP address and host name of the machine	
--	---	--

The following sections describe the procedure for each operation separately.

3.7.1 Backing Up the Server Database

Note: If you upgraded Device Manager from version 3.5 or earlier to version 4.0 or later, the menu options (**Start**, **Programs**, **HiCommand**, **Device Manager**, and **Back Up Database**) are deleted.

Caution: To back up the Device Manager database, a folder for storing the backup file is required. The capacity of this folder must be at least the total size of the following two folders:

- The folder storing the Device Manager database
- The folder storing the HiCommand Suite Common Component database

This capacity is a guideline value applied when only the Device Manager database is installed. If HiCommand Suite products other than Device Manager are also installed, take the capacities of those databases into account as well.

To back up the database:

1. Stop the Device Manager Server:

Select **Start → Programs → HiCommand → Device Manager → Stop Server**.

2. Enter the following command from the command prompt to make sure that HiRDB is running:

<common component installation folder>\Bin>hcmdssrv /status.

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /status

Several messages are displayed. If the following message is one of them, HiRDB is running normally:

KAPM06440-I The HiRDB service has already started.

3. If HiRDB is not running, execute the following command from the command prompt:

<common component installation folder>\bin\hcmdssrv /start

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start

4. Execute the **hcmdsbbackups** command from the command prompt:

<common component installation folder>\bin\hcmdsbbackups.bat

The command format is as follows:

hcmdsbbackups -dir target-folder-for-storing-backup-files

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmsgbackups /dir C:\db_bkup01

The specifiable option is as follows:

dir

Specify the absolute path of the folder that stores backup files of the Device Manager Server database. Be sure to specify an empty folder, or the process will be aborted. If that occurs, specify an empty folder and then re-execute the command.

Note: When you execute the **hcmsgbackups** command, a folder named **database** will be created in the target folder for storing backup files, and the database backup file will be stored with the name **backup.hdb**.

5. Restart the Device Manager Server:

Select **Start → Programs → HiCommand → Device Manager → Start Server**

3.7.2 Restoring the Server Database

WARNING: Before restoring the database, be sure to confirm that the following are the same in the backup source Device Manager server and the restore destination Device Manager server. If the following are not the same, the database cannot be restored.

- Types, versions, and revisions of the installed HiCommand Suite products
- Installation location for each HiCommand Suite product, HiCommand Suite Common Component, each HiCommand Suite product database, and HiCommand Suite Common Component database
- The IP address and host name of the machines

Caution: When the HiCommand Device Manager server is upgraded from version 3.5 or earlier to 4.0 or later, the menu options (**Start**, **Programs**, **HiCommand**, **Device Manager**, and **Restore Database**) are deleted

To restore a database:

1. Stop the Device Manager Server and the Common Component as follows:

Select **Start → Programs → HiCommand → Device Manager → Stop Server with Common Services**

2. Execute the **hcmsgdb** command from the command prompt. The default destination for this command is as follows:

<Common Component installation folder>\bin\hcmsgdb.bat

The command format is as follows:

hcmsgdb -restore backup-file /type DeviceManager

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmsgdb /restore
C:\db_bkup01\backup.hdb /type DeviceManager
```

The specifiable options are as follows:

- **/restore**: Specify the absolute path of the Device Manager Server database backup file (backup.hdb).
- **/type**: Specify the name of the HiCommand Suite product to be restored. Specify **DeviceManager** to restore the Device Manager database only, or specify **ALL** (all capital letters) if you want to restore all HiCommand Suite product databases at once. Specify **ALL** if you want to restore the databases when you are uninstalling and then reinstalling all the HiCommand Suite products.

Note: If you specify **DeviceManager** for the type option, specify **true** for the **server.base.initialsynchro** property in the server.properties file. See section 8.2.23 for more information.

Note: This sample command used the C:\TMP directory as the backup location. Use the backup location that you previously specified.

3. Following the **hcmdsdb** command execution, restart the Device Manager Server:
Select **Start → Programs → HiCommand → Device Manager → Start** Server with Common Services

3.7.3 Migrating the Server Database

If HiCommand Suite products are used for an extended period of time, you may need a higher performance machine in order to accommodate product version upgrades and the increased number of objects to be managed. If this occurs, database migration will be one important component of the machine replacement process. In HiCommand Suite products, you can migrate the database by using the **hcmdsdbtrans** command. The **hcmdsdbtrans** command migrates all information stored in the database of each HiCommand Suite product as well as user information managed by the HiCommand Suite Common Component.

You can use the **hcmdsdbtrans** command to migrate the Device Manager database to a machine that has a different environment than the currently operating server machine, as shown in the following cases:

- Migration to a different platform machine
- Migration to a machine on which the installation locations for HiCommand Suite products are different from the ones on the migration source
- Migration to a machine on which the versions of HiCommand Suite products are newer than the ones on the migration source

3.7.3.1 Notes When Migrating the Database

The following are notes for the types, versions, and user information of the HiCommand Suite products on the migration source and migration destination servers.

Notes for types and versions of the HiCommand Suite products on the migration source and migration destination servers:

- The database of a HiCommand Suite product that is not installed on the migration destination server cannot be migrated. Install all necessary HiCommand Suite products on the migration destination server.

- If any of the versions of the HiCommand Suite products installed on the migration destination server is older than the ones on the migration source server, the database cannot be migrated. On the migration destination server, install the HiCommand Suite products whose versions are the same as or higher than the ones on the migration source server.
- The database of Replication Monitor version 4.2 cannot be migrated. If you need to migrate this database, upgrade the Replication Monitor to version 5.0 or later on both the migration source and destination servers beforehand.

Notes for user information:

- If there is user information on the migration destination server, this user information will be replaced with the user information from the migration source server. Therefore, do not perform a migration to the machine on which user information for the HiCommand suite products already exists.
- If the databases of several HiCommand Suite products installed on a management server are migrated in multiple operations, the user information is replaced with new information at each operation, and eventually only the user information for the products migrated during the last operation will remain. When you perform migration for multiple products, be sure to migrate the databases in one operation so that user information for every products can be migrated.
- You cannot perform migration to integrate the HiCommand Suite products that were running on multiple management servers on to one management server because user information will be overwritten with each successive migration.

3.7.3.2 Procedure for Migrating Databases

To migrate databases:

1. Install, on the migration destination server, the HiCommand Suite products whose databases will be migrated.
2. Export the databases at the migration source server by using the `hcmdsdbtrans` command.
3. Transfer the archive file from the migration source server to the migration destination server.
4. Import the database at the migration destination server by using the `hcmdsdbtrans` command.

The following sections describe the details of each procedure. To perform migration between heterogeneous platforms, also see section 4.8.3.

3.7.3.3 Installing the HiCommand Suite Products on the Migration Destination Server

Install, on the migration destination server, the HiCommand Suite products whose databases will be migrated. The version of each HiCommand Suite product installed on the migration destination server must be the same as or higher than the one on the migration source server.

3.7.3.4 Exporting the Database at the Migration Source Server

To export the database of Device Manager, a folder for temporarily storing the information of the database, and a folder for storing the archive file are required. Each of these folders requires the as much capacity as the total size of the following two folders:

- The folder storing the Device Manager database
- The folder storing the HiCommand Suite Common Component database (excluding the `SYS` folder and the folders beneath it)

This capacity is a guideline value applied when only the Device Manager database is installed. If HiCommand Suite products other than Device Manager are also installed, take the capacities of those databases into account as well.

Caution: If the total capacity of the database exceeds 2 GB, an attempt to create the archive file fails when the database is exported. In this case, instead of using the archive file, transfer to the migration destination the database information collected when exporting the database.

To export the database at the migration source server:

1. Stop the Device Manager server and HiCommand Suite Common Component using the following procedure:

Select **Start, Programs, HiCommand, Device Manager, Stop Server with Common Services**.

Important: If other HiCommand Suite products are running, stop them all.

2. From the command prompt, execute the following command to start HiRDB:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbsrv /start
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
```

3. From the command prompt, execute the `hcmdsdbtrans` command.

The default installation location of the `hcmdsdbtrans` command is as follows:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbtrans
```

The command format is as follows:

```
hcmdsdbtrans /export /workpath working-folder /file archive-file
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbtrans /export /workpath D:\trans_work /file D:\trans_file \db_arc
```

In the `hcmdsdbtrans` command, you can specify the following options:

`workpath`

Specify the absolute path to the folder where you wish to temporarily store database information. Specify a folder on your local disk.

Caution: Specify an empty folder for the `workpath` option. If you specify a folder other than an empty folder, export processing will be cancelled. If this occurs, specify an empty folder and execute the `hcmdsdbtrans` command again.

file

Specify the absolute path to the archive file of the database to be exported.

The following table lists the actions to be taken when an error message is output. If a message that does not have one of the following message IDs is output, take actions according to the message.

Table 3.13 Action to Be Taken When an Error Message Is Output (During an Export)

Message ID	Action
KAPM05909-E	Collect maintenance information, and then contact Customer Support.
KAPM05910-E	Make sure that the products have been properly installed, and if necessary, take actions to satisfy this condition. If an error still occurs after taking the above actions, collect maintenance information, and then contact Customer Support.
KAPM05922-E	Make sure that you secure sufficient space in the disk that is to store the archive file. If an error still occurs even after securing the disk space, collect maintenance information, and then contact Customer Support.
KAPM05923-E	Instead of the archive file, transfer the data stored in the folder specified by the <code>workpath</code> option to the migration destination server.

4. Transfer the exported file to the migration destination server.

If the archive file cannot be created, transfer all the files stored in the folder specified by the `workpath` option. In that case, do not change the file structure in the folder specified by the `workpath` option.

3.7.3.5 Importing the Database at the Migration Destination Server

Caution: If the OS of the migration destination server is Solaris or Linux, follow the procedure in section 4.8.3.5.

To import the database at the migration destination server:

1. Stop the Device Manager server and HiCommand Suite Common Component as follows:

Select **Start, Programs, HiCommand, Device Manager, Stop Server with Common Services**.

Important: If other HiCommand Suite products are running, stop them all.

2. From the command prompt, execute the following command to start HiRDB.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbsrv /start
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
```

3. From the command prompt, execute the `hcmdsdbtrans` command.

The default installation location of the `hcmdsdbtrans` command is as follows:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbtrans
```

The format of the command is as follows:

```
hcmdsdbtrans /import /workpath working-folder [/file archive-file] /type {ALL |  
HiCommand-Suite-products-whose-databases-will-be-migrated}
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbtrans /import /workpath D:\trans_work /type ALL
```

In the `hcmdsdbtrans` command, you can specify the following options:

`workpath`

When using an archive file during the import:

Specify the absolute path to the folder used to extract the archive file. Specify a folder on your local disk. If you use an archive file, the `file` option must be specified.

Caution: Specify an empty folder for the `workpath` option. If you specify a folder other than an empty folder, export processing will be cancelled. If this occurs, specify an empty folder, and then execute the `hcmdsdbtrans` command again.

When not using the archive file during the import:

Specify the folder that stores the database information transferred from the migration source server. Do not change the file structure in the transferred folder. Also, do not specify the `file` option.

`file`

Specify the absolute path to the archive file of the databases transferred from the migration source server. If the database information transferred from the migration source server is stored in the folder specified by `workpath`, you do not need to specify this option.

`type`

Specify the names of the HiCommand Suite products whose databases will be migrated. Only the databases of the specified products are migrated.

You can use the `type` option to migrate the databases only when the databases of all the specified products exist in the folder specified by the archive file or the `workpath` option, and all the specified products are installed on the migration destination server. If any of the products do not meet the conditions above, migration will not performed.

The following product names can be specified: `DeviceManager`, `GlobalLinkAvailabilityManager`, `ReplicationMonitor`, `TieredStorageManager`, and `TuningManager`. To specify multiple product names, use a comma as the delimiter between the names.

To migrate the databases of all the installed HiCommand Suite products at a time, specify `ALL`. The databases of the HiCommand Suite products installed on the migration destination server are automatically selected and migrated.

Caution: If Replication Monitor version 4.2 is installed on the migration source machine, you cannot migrate the database. Therefore, upgrade Replication Monitor on the migration source and migration destination machines to version 5.0 or later, and then perform migration. If Replication Monitor cannot be upgraded to version 5.0 or later, or the Replication Monitor database does not have to be migrated, use the `type` option and specify all products other than Replication Monitor when you execute the command.

The following table lists the actions to be taken when an error message is output. If a message that does not have one of the following message IDs is output, take actions according to the message.

Table 3.14 Action to Be Take When an Error Message Is Output (During an Import)

Message ID	Action
KAPM05909-E	Collect maintenance information, and then contact Customer Support.
KAPM05910-E	Make sure that the products have been properly installed, and if necessary, take actions to satisfy this condition. If an error still occurs after taking the above actions, collect maintenance information, and then contact Customer Support.
KAPM05911-E	Check the version of the products. If migration is not supported for the version of the products, use the <code>type</code> option to import all products other than the unsupported products.
KAPM05913-E	Perform one of the following operations: - Install the products that are not installed on the migration destination. - Use the <code>type</code> option to import only the products installed on the migration destination.
KAPM05914-E	Use the <code>type</code> option to specify only the products that are included in the archive file or in the folder specified by the <code>workpath</code> option.
KAPM05915-E	Check the data to be imported.
KAPM05916-E	Check the data to be imported and the setting of the server to which the data is to be imported.
KAPM05921-E	Make sure the following conditions are satisfied, and if necessary, take actions to satisfy them: The capacity of the disk used for the folder specified by the <code>workpath</code> option is sufficient. The archive file is for the <code>hcmsdbtrans</code> command. If an error still occurs after taking the above actions, collect maintenance information, and then contact Customer Support.
KAPM05926-E	- When the <code>file</code> option is specified Check whether the specified file is the archive file for the <code>hcmsdbtrans</code> command. - When the <code>file</code> option is not specified Check whether all the contents of the folder specified by the <code>workpath</code> option when exporting are stored in the folder specified by the <code>workpath</code> option. If an error still occurs after taking the above actions, collect maintenance information, and then contact Customer Support.

4. Synchronize the repository information with the imported Device Manager database information.

Specify `true` for the `server.base.initialsynchro` property in the `server.properties` file.

Since, other than user information, the `hcmsdbtrans` command does not migrate the HiCommand Suite Common Component repository, you need to synchronize the repository information with the database information of the imported Device Manager.

For information on the `server.base.initialsynchro` property, see section 8.2.22.

5. Restart the Device Manager server and HiCommand Suit Common Component on the migration destination as follows:

Select **Start, Programs, HiCommand, Device Manager, Start Server with Common Services**.

3.7.4 Initializing a HiCommand Device Manager Server Database

To initialize the database:

1. Stop the Device Manager Server:

Select **Start → Programs → HiCommand → Device Manager → Stop Server**

2. Verify that HiRDB is running:

<common component installation folder>\bin\hcmdssrv /status

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /status

If the following message is displayed, HiRDB is running normally:

KAPM06440-I The HiRDB service has already started.

3. If HiRDB is not running, execute the following command from the command prompt:

<common component installation folder>\bin\hcmdssrv /start

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /start

4. From the command prompt, execute the **database** command.

- The default installation location is as follows:

<server installation folder>\database.bat

- The following shows an example of executing the command:

C:\Program Files\HiCommand\DeviceManager\database initialize

- The command format is as follows: **database initialize**

5. Specify **true** for the **server.base.initialsynchro** property in the server.properties file. For details, see section 8.2.23.

6. Restart the Device Manager Server:

Select **Start → Programs → HiCommand → Device Manager → Start Server**

7. In the server.properties file, change the **server.base.initialsynchro** property back to false. See section 8.2.23 for more information.

3.8 Uninstalling the HiCommand Device Manager Server and Related Products

3.8.1 Uninstalling the HiCommand Device Manager Server in a Standard Environment

WARNING: Unless you are experiencing problems and need to redo a complete installation, you should not uninstall Device Manager. If you need to uninstall the Device Manager Server, make sure to first back up your configuration (see section 3.7.1 for instructions).

WARNING: The Device Manager provides user management functions for the HBase Storage Mgmt Common Service. When you are using the HBase Storage Mgmt Common Service function, and Device Manager Server and Tuning Manager are installed on the same machine, the HBase Storage Mgmt Common Service function is deleted when Device Manager is uninstalled.

Notes:

- Files that were added to the installation folder after installation might not be deleted when you uninstall. If this occurs, delete the files manually.
- If services and files remain after uninstallation, If this type of problem occurs, delete the **<install directory>\UninstallerData** folder, re-install Device Manager, and then uninstall again.
- If no other program is using the Common Component, it will be uninstalled during the uninstallation of Device Manager. If another program is using the Common Component, it will remain installed. You cannot uninstall the Common Component by itself.
- When you uninstall Device Manager, the directories or files under *installation-folder-for-the-Device-Manager-server* will be deleted. The files will be deleted, but the directory itself will remain after the uninstallation. If the directory is not necessary, you can delete it manually. Note that certain files that remain may be in use by another HiCommand product.
- Even though InstallAnywhere® indicates that it uninstalls all components that were installed by that program, only the Device Manager Server will actually be uninstalled.
- The Uninstaller is executed in the same language display as the language that was selected during the original Device Manager installation. If the original installation was performed in one language, but the system local parameters were later modified to another language and the uninstallation processing is performed in the second language, then the characters on the Uninstaller screen will be garbled.
- If CIM/WBEM functions are being used, you must release the registration of the SLP service from the Windows service before performing the uninstallation. For details about releasing an SLP service registration, see the *HiCommand Device Manager CIM/WBEM User's Guide*.
- **Caution:** Open the property of the following services from the Services panel to make sure that **Startup Type** is not set to **Disabled**. If **Startup Type** is set to **Disabled**, change the setting to **Automatic** or **Manual**.
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service

- HiRDB/EmbeddedEdition_HD0
- HiCommandServer
- **Caution:** Check whether the following programs are installed. If they are installed, take action by following the explanation below:
 - A program that monitors security

Stop the program that monitors security, or change its settings so that Device Manager can be uninstalled normally.
 - A program that detects viruses

We recommend that you stop programs that detect viruses, and then uninstall Device Manager.

If a program that detects viruses is running during uninstallation of Device Manager, the speed of uninstallation might be reduced, uninstallation might fail, or uninstallation might finish in an incorrect state.
 - A program that monitors processes

Stop the program that monitors processes, or change its settings so that the program does not monitor the services or processes of the HiCommand Device Manager server and the HiCommand Suite Common Component.

If a program that monitors processes starts or stops the above services or processes during uninstallation of Device Manager, uninstallation might fail.
- **Caution:** Any user who is not a member of the Administrators group can uninstall the HiCommand Device Manager server. If this is not desirable, change the security settings in the following file to prevent uninstallation by other users:

```
<device manager server installation
folder>\UninstallerData\Uninstall_HiCommand.exe
```

- **Caution:** Sometimes, even when a message has notified you that uninstallation was successful, uninstallation has actually failed. For example, the HiCommandServer service and some installation files may remain. If uninstallation has failed, manually delete the *installation-folder-for-the-Device-Manager-server\UninstallerData* folder, re-install the HiCommand Device Manager server program, and then perform uninstallation again.
- **Caution:** When you uninstall HiCommand Device Manager from a computer on which another HiCommand Suite product is installed, the **GO** menu command for launching Device Manager remains on the dashboard of that program. To remove **GO**, a user with User Management permissions must execute the following command. When this command is executed, the HiCommand Suite Common Component services must be running.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsintg /delete /type
DeviceManager /user user-ID /pass password
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsintg /delete /type DeviceManager /user dvmuser1
/pass sys0305
```

To uninstall the HiCommand Device Manager server:

1. Stop any other HiCommand Suite software that is running (for example, Tuning Manager).
2. Access the **Uninstall HiCommand Device Manager** panel using one of the following:
 - The Windows Add/Remove Programs utility
 - Select **Start → Programs → HiCommand → Device Manager → Uninstall Device Manager**
3. When the HiCommand Suite Common Component services are running, the Stop HiCommand Suite Common Component Services panel is displayed. Select **OK** to continue.

If the uninstaller cannot stop the HiCommand Suite Common Component services, the HiCommand Suite product is running panel is displayed, and the uninstallation stops. Stop the HiCommand Suite Common Component services manually, and then perform the uninstallation again.

4. After the message `All items were successfully uninstalled.` is displayed, select **Done** to exit. OS indicates that certain files were not uninstalled, you must manually delete them.

WARNING: If you uninstall HiCommand Suite Common Component, the Warning Panel shown in Figure 3.12 may display. In this case, you need to restart the system after the uninstallation. If you install a HiCommand Suite product continuously without restarting the system after the uninstallation, when the system restarts after the installation, the files required for the HiCommand Suite product operations will be deleted.

Caution: If the following message is displayed, release the SLP service from the Windows services manually. If the folders and files that are related to the SLP remain, delete them manually as necessary. For information on how to release the SLP service, see section 11.5.1.1.

An attempt to release the SLP service has failed. After uninstallation, release the SLP service manually.
Uninstallation continues

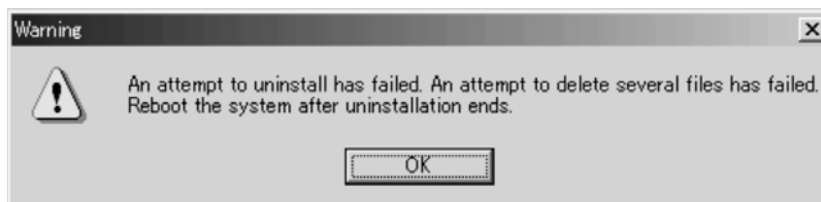


Figure 3.12 Warning Panel

3.8.2 Uninstalling the Device Manager Server in a Cluster Environment

This section assumes that that Device Manager is installed in the default installation folder of the c: drive in both the active and standby nodes, and that the active node recognizes the shared disk of the active and standby nodes as the r: drive.

Caution: If the service is not online on the executing node, first place it online, and then perform the uninstall procedure.

To uninstall the HiCommand Device Manager Server in a Microsoft Cluster Service environment, perform the following procedure:

1. Open the cluster administrator:

Select **Start → Settings → Control Panel → Administrative Tools → Cluster Administrator**.

2. Place the following services offline:

- HiCommand Server
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service

The above services are represented by the resource names registered in section 3.3.3.3.

3. On the executing node, stop the Common Component:

<common component installation folder>\bin\hcmdssrv /stop

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

4. Place the **HiRDB** service offline.

The above service is represented by the resource name registered in section 3.3.3.3.

5. If the following resources are not in use by another application, delete them:

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- HiCommandServer
- HiRDB

The above services are represented by the resource names registered in section 3.3.3.3.

6. For those services that you did not delete, in the Cluster Administrator, right-click each service, select **Properties**, select the **Advanced** tab, select **Do not restart**, and then select **OK**.

7. On the executing node, uninstall the Device Manager Server by selecting **Start, Programs, HiCommand, Device Manager**, and then **Uninstall Device Manager**.

8. On the executing node, delete any files and folders that are no longer necessary, including those created during the installation in the cluster environment.

9. Place the group to which the HiCommand Device Manager service has been registered on standby.

10. In the Cluster Administrator, right-click the group to which the HiCommand Device Manager service has been registered, and then choose **Move Group**.

11. On the standby node, uninstall the Device Manager Server by selecting **Start, Programs, HiCommand, Device Manager**, and then **Uninstall Device Manager**.
12. On the standby node, delete any files and folders that are no longer necessary, including those created during the installation in the cluster environment.
13. If the following resources are not being used by another application, first place the corresponding resource offline, and then delete it:
 - IP address
 - Shared disk
14. If the group where the HiCommand Device Manager resources are registered is no longer necessary, delete that as well.
15. Change those services that you previously set as **Do not restart** to **Restart**.

3.8.3 Uninstalling InterBase Server and Client

WARNING: Do not uninstall InterBase Server if it is being used by another product, on the same machine, including another HiCommand Suite product that has not yet been upgraded to version 4.0 or higher.

To uninstall InterBase Server:

1. Stop the Device Manager Server:
Select **Start → Programs → HiCommand → Device Manager → Stop HiCommand**.
WARNING: Do not use the **Services** panel to stop the Device Manager Server.
2. Access the **Services** Panel.
3. Select **InterBase Guardian → Stop**.
4. The **Microsoft Management Console** displays. Select **OK** to continue.
Note: If the InterBase Guardian service cannot be stopped, an error message appears (see Figure 3.13). Select **OK** to continue.
5. Use the Windows **Add/Remove Programs** utility to remove the entries for the InterBase software (the exact details are determined by your existing configuration).
6. The InterBase uninstallation program may leave a directory structure on your system. The default location is c:\Program Files\Borland\InterBase. You can delete the directories manually if they are no longer necessary.
7. After the uninstallation, select the **View Log** button on the uninstaller to make sure that no errors occurred.
8. Reboot the system. If you are also going to uninstall the InterClient software, the reboot can wait until after InterClient is uninstalled.

Notes:

If the uninstallation fails, retry the operation. If it fails again, restart the machine, re-install the InterBase Server, and then uninstall the InterBase Server again.

After you uninstall InterBase Server, you must restart the system before you re-install the Device Manager Server.



Figure 3.13 Microsoft Management Console Error Message 997

3.8.4 Uninstalling InterClient

WARNING: Do not uninstall InterClient if it is being used by another product, including another HiCommand Suite product that has not yet been upgraded to version 4.0 or higher.

To uninstall the InterClient software:

1. Before you uninstall InterClient, stop the service by accessing the **Services** Panel, then select **Interserver** → **Stop**.
2. Choose **Start, Programs, InterBase InterClient**, and then **InterServer Configuration Utility**.
3. Choose the **Advanced** tab, and then click the **Remove** button. A message asking whether you want to delete the service appears.
4. Click the **OK** button.
5. From the `services` file (`system-folder\system32\drivers\etc\services`), delete the following line:

interserver	3060/tcp	# InterBase InterServer
-------------	----------	-------------------------

6. Use the Windows **Add/Remove Programs** utility to remove the InterClient software (the exact details are determined by your existing configuration).
7. The InterClient uninstallation program may leave a directory structure on your system. The default location is **c:\Program Files\Borland\InterClient**. You can delete the directories manually if they are no longer necessary.

Notes:

- If the InterClient software is uninstalled, you must restart before you can re-install.
- If the uninstallation fails, retry the operation.

Chapter 4 Solaris and Linux Systems Installation

This chapter contains instructions for installing the Device Manager Server software on a single central server system. For instructions on installing and using the graphical Web Client software, see the *HiCommand Device Manager Web Client Installation and Configuration Guide*.

This chapter discusses the following topics:

- Installation Prerequisites for Solaris Systems (see section 4.1)
- Managing the LUN and Security Counts (see section 4.2)
- Preparing for Installation to a Solaris Environment (see section 4.3)
- Installing Device Manager Server and Common Component (see section 4.4)
- Installing the Device Manager Server in a Cluster Server Environment (see section 4.5)
- Verifying HiCommand Device Manager Installation (see section 4.6)
- Starting and Stopping Device Manager Server (see section 4.7)
- Operating the HiCommand Device Manager Server Database (see section 4.8)
- Converting a Device Manager Server Database (see section 4.9)
- Uninstalling Device Manager Components (see section 4.10)
- Uninstalling the HiCommand Device Manager Server and Related Products (see section 4.11)
- Setting Kernel Parameters on Solaris (see section 4.12)
- Setting Kernel Parameters and Shell Restrictions on Linux (see section 4.13)

4.1 Installation Prerequisites for Solaris Systems

4.1.1 Solaris and Linux System and Media Requirements

The following are the system requirements for Sun™ Solaris and Linux systems:

- Solaris workstation: SPARC™
- Operating system:
 - The following Solaris versions are supported:

Table 4.1 The OSs on Which the HiCommand Device Manager Server Can Run (Solaris)

Abbreviated name	Full name
Solaris 8 or Solaris ^{#1}	Sun Microsystems Solaris 8 (for SPARC)
Solaris 9 or Solaris	Sun Microsystems Solaris 9 (for SPARC)

Solaris 10 or Solaris ^{#2}	Sun Microsystems Solaris 10 (for SPARC) ^{#3}
-------------------------------------	---

#1 The following patches are required:

Patch Cluster, 108652-59, 111293-04, 108714-07, 108827-30

#2 Patch 120664-01 is required.

#3 The HiCommand Device Manager server runs in the usual global environment (global zone) only. If a non-global zone has been created, install the HiCommand Device Manager server in the global zone.

- The following Linux versions are supported:

Table 4.2 The OSs on Which the HiCommand Device Manager Server Can Run (Linux)

Abbreviated name	Full name
Linux	Red Hat Enterprise Linux AS 4.0 Update1 ^{#1#2}
	Red Hat Enterprise Linux ES 4.0 Update1 ^{#1#2}

#1 Only x86 versions are supported.

#2 The `compat-libstdc++-33-3.2.3-47.3` library must be installed. Make sure that the `compat-libstdc++-33-3.2.3-47.3` library is installed before you install the Device Manager server.

■ Machine specifications:

- Recommended specifications for Solaris machines are as follows:

Table 4.3 Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed (Solaris)

Item	Minimum	Recommended
Processor	1.0 GHz	1.2 GHz or faster
Memory	1 GB	At least 2 GB [#]
Disk space	4 GB	At least 5 GB

- Recommended specifications for Linux machines are as follows:

Table 4.4 Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed (Linux)

Item	Minimum	Recommended
Processor	1.0 GHz	2.0 GHz or faster
Memory	1 GB	At least 2 GB [#]
Disk space	4 GB	At least 5 GB

When the HiCommand Device Manager server is used concurrently with other software products, the memory requirements of all of the software products must be taken into account.

- Installation destination and its disk space requirements: The following table describes the installation paths and the required disk space for installation.

Table 4.5 Installation Path and Required Disk Space

Item	Installation path	Required disk space (GB)
Installation destination for the HiCommand Device Manager server	/opt/HiCommand	1.30
Installation destination for HiCommand Suite Common Component	/opt/HiCommand/Base	
	/var/opt/HiCommand/Base	0.01
Storage destination of the database for the HiCommand Device Manager server	/opt/HiCommand/HiCommandServer/database	0.10
Storage destination of the database for HiCommand Suite Common Component ^{#1}	/var/opt/HiCommand/Base/database	1.20
A temporary directory ^{#2}	/var/tmp	1.30

#1 This is not required if HiCommand Suite Common Component version 4.0 or later has already been installed.

#2 This is temporarily required during installation. However, this will be unnecessary after finishing installation.

- Prerequisite programs: J2SE Java Runtime Environment 1.4
The JRE is installed automatically when you install the HiCommand Device Manager server.
- CD-ROM drive
- Static IP address (used to test the LAN connections and allow access to the Device Manager Server)
- Device Manager Server residing on the same network as the storage subsystem(s)
- The HiCommand Device Manager server only supports IPv4 (it does not support IPv6). Connect the HiCommand Device Manager server, Web Client, the HiCommand Device Manager agent, and a storage subsystem by using IPv4. For details about how to disable IPv6, refer to the appropriate documentation for each OS.

- The following package for unpacking the installer (which has been packed by using gzip)
For Solaris: SUNWgzip
For Linux: gzip
- LAN cables, connections to the storage subsystem, and a 10/100 Ethernet LAN card that has TCP/IP installed and available. (If the machine and the LAN cable are compatible with Gigabit Ethernet, you can use a Gigabit-class card.)

WARNING: Do not install Tuning Manager version 4.0 or higher on the same server as Device Manager version 4.0 or higher.

WARNING: Do not install Device Manager and Hitachi Storage Services Manager on the same server.

Caution: HiCommand Device Manager does not support operations that use the terminal service function.

Important: The Device Manager Server and Agent must have the same version to be able to communicate with each other.

Always read the Release Notes before installing Device Manager, and make sure that you have the minimum required microcode on the subsystem.

4.2 Managing the LUN and Security Counts

The following table shows the maximum number of resources that can be managed by the HiCommand Device Manager server. We recommend that you operate the HiCommand Device Manager server within these limits. The default value in the table is used if you do not change the operation environment settings (the memory heap size settings) of HBase Storage Mgmt Web Service:

Table 4.6 Maximum Number of Resources Managed by the HiCommand Device Manager Server

Resource		When using report function		When not using report function	
		Maximum value for the entire Device Manager	Maximum value for one storage subsystem	Maximum value for the entire Device Manager	Maximum value for one storage subsystem
Number of LUNs	Maximum setting	20,000	20,000	100,000	32,000
	Default	15,000	15,000	32,000	32,000
Number of Securities	Maximum setting	30,000	30,000	150,000	48,000
	Default	20,000	20,000	48,000	48,000
Number of LDEVs	Maximum setting	10,000	10,000	50,000	16,000
	Default	7,500	7,500	16,000	16,000

In an environment in which HiCommand(R) Device Manager is used, if the assumed number of resources exceeds the default setting, estimate the number of managed resources by using the formula shown below.

When multiple storage subsystems are to be managed, estimate the number of managed resources for each storage subsystem, and use the greatest value as a guideline.

Formula:

$$\begin{aligned} \text{number-of-managed-resources} &= \text{number-of-LDEVs} \times 2.5 + \text{total-number-of-paths}^\# \\ \# \text{ total-number-of-paths} &= \text{number-of-LDEVs} \times \text{average-number-of-paths-per-LDEV} \end{aligned}$$

If the *number-of-managed-resources* is 28,000 or greater or if an *Out Of Memory* error occurs while you are using Web Client to perform an operation such as displaying a list of LDEVs, use the following procedure to set the memory heap size:

1. Execute the following command to stop the HiCommand Device Manager server and HiCommand Suite Common Component:

```
# /opt/HiCommand/suitesrvctl -stop_all
```

2. Set the memory heap size as follows:

```
# /opt/HiCommand/Base/bin/hcmdsweb -add -file
/opt/HiCommand/HiCommandServer/webapps/DeviceManager.war -server
HiCommand -javaoption HDvM.serverpath=/opt/HiCommand -nolog -type
DeviceManager -Xms256 -Xmx512
```

3. Restart the Device Manager Server and Common Component as follows:

```
# /opt/HiCommand/suitesrvctl -start_all
```

Note: When using one HiCommand Device Manager server, it is not possible to use separate storage partitions with different storage administrator accounts. If you want to manage individual storage partitions, a HiCommand Device Manager server is required for each storage partition.

Caution: If CIM/WBEM functions are being used, you might have to increase the memory heap size, depending on the conditions.

To change the memory heap size:

1. Edit the `hicommand.sh` file in the following directory to change the memory heap size:

```
/opt/HiCommand
```

2. Open the `hicommand.sh` file in a text editor, and change the value of the `-Xmx` option of the `java` command specified in the `start` option script to *new-setting-value* (units: MB) in the formula below. Note that if the value of *calculation-value-for-SMI-S-Provider* is smaller than 256 MB, use 256 MB as the value of *calculation-value-for-SMI-S-Provider* and then calculate the value of *new-setting-value*.

$$\text{calculation-value-for-SMI-S-Provider} = 30000 \times \text{number-of-LDEVs} \times \text{number-of-paths} / 1048576^\#$$

$$\text{new-setting-value} = \text{current-setting-value} + \text{calculation-value-for-SMI-S-Provider}$$

To be rounded up after the decimal point

3. The following shows how to change the value if the *new-setting-value* is calculated to be 512 MB.

Before: `java -Xmx256m -classpath ...`

After: `java -Xmx512m -classpath ...`

4. After the `hicommand.sh` file is changed, perform the following to restart the Device Manager server.

Execute the following command:

```
# /opt/HiCommand/suitesrvctl -stop_hdvm
```

After the Device Manager server has stopped, execute the following command:

```
# /opt/HiCommand/suitesrvctl -start_hdvm
```

4.3 Preparing for Installation to a Solaris Environment

Device Manager Server will be installed in **/opt/HiCommand**.

The Common Component will be installed in **/opt/HiCommand/Base**.

4.3.1 Preparing for Installation

Before you start installation, check the usage status of the port numbers, the installation status of other programs, and other information as described below.

4.3.1.1 Checking Port Numbers

Check whether the port numbers required to use HiCommand Device Manager are being used by another product on the machine on which the HiCommand Device Manager server is to be installed by using the `netstat` command.

Example: Check whether another program is using the port 162/udp.

Execute the following command:

In Solaris: `netstat -an -P udp`

In Linux: `netstat -uan`

The following shows an example of executing the command in Solaris:

```
# netstat -an -P udp | more
```

UDP						
Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
.	*.*	0	0	0	0	IDLE
*.111	*.*	0	0	0	0	LISTEN
.	*.*	0	0	0	0	IDLE
*.389	*.*	0	0	0	0	LISTEN

In the command execution results, if there are no lines in which 162 for Local Address, and LISTENING for State appears, the port is not being used.

Also, make sure that the following file does not contain a 162/udp description:

```
/etc/services
```

The following shows the ports required to use HiCommand Device Manager. For details about the intended use of each port, see section 2.4 and section 5.4.1.

Port numbers that must be checked

- From 23015 to 23018, and 23032: If another product is using any of these ports, change the settings of that product, or change the settings of HiCommand Device Manager. For details about how to change these port numbers, see section 5.4.2. If HiCommand Suite Common Component has been installed and these ports have been changed, you can install the HiCommand Device Manager server by using those ports. You do not need to set up the default ports.
- From 45001 to 49000: For these port numbers, the settings of HiCommand Device Manager cannot be changed. Therefore, you need to change the settings of any other products that are using the same ports as HiCommand Device Manager.
- 2001: If another product is using this port number, change the settings of that product, or change the port number to be used before HiCommand Device Manager starts. For details about how to change this port number, see section 8.2.2. If another product is using this port number, HiCommand Device Manager will not be able to start, and the following message will be output to the application log and sys log: KAIC00114-E An attempt to start the HTTP server on port "2001" failed.

Port numbers that must be checked when some functions are enabled

- 162: This port number is used when the SNMP Trap reception function of HiCommand(R) Device Manager is enabled. To disable the SNMP Trap reception function, select disable in the Setting for the SNMP Trap Reception Function panel during installation (see Figure 4.8).
- 1099: This port number is used when the function to link with Storage Navigator Modular (for Web) (see section 9.1), or DAMP (for Web) (see section 9.1.4) is enabled. For details about how to change the port number used to link with Storage Navigator Modular (for Web), see section 9.1.2. The port number for the function to link with DAMP (for Web) cannot be changed. When the port number 1099 is used by another product, perform one of the following operations so that other products do not use the port number 1099 at the same time as HiCommand Device Manager.

If a product that uses the port number 1099 is always running, use different machines to run HiCommand Device Manager and that product respectively.

If a product that uses the port number 1099 runs temporarily, restart DAMP (for Web).

- 2000: This port number is used when the function to link with Storage Navigator Modular (for Web) (see section 9.1) or DAMP (for Web) (see section 9.1.4) is enabled. For details about how to change this port number, see section 1.5.1.1 or 1.5.1.5.
- 2443: This port number is used when SSL communication is enabled. For details about how to change this port number, see section 8.2.3. If another product is using this port number, the following message will be output to the application log and sys log and HiCommand Device Manager will not be able to start: KAIC00115-E An attempt to start the HTTPS server on port "2443" failed.

4.3.1.2 Checking Other Programs Related To Security

- Check whether the following programs are installed. If they are installed, take action by following the explanation below:
 - A program that monitors security
Stop the program that monitors security, or change its settings so that Device Manager can be installed normally.
 - A program that detects viruses
We recommend that you stop programs that detect viruses, and then install Device Manager.

If a program that detects viruses is running during installation of Device Manager, the speed of installation might be reduced, installation might fail, or installation might finish in an incorrect state.
 - A program that monitors processes
Stop the program that monitors processes, or change its settings so that the program does not monitor the processes of the HiCommand Device Manager server and the HiCommand Suite Common Component.

If a program that monitors processes starts or stops the above processes during installation of Device Manager, installation might fail.

4.3.1.3 Checking Other Programs

- HiCommand Device Manager cannot be installed on the server on which Tuning Manager has been installed with a Large configuration. If you try to install HiCommand Device Manager in such an environment, the installation is canceled. If that happens, install Tuning Manager and HiCommand Device Manager separately on different servers.
- You cannot install a version of Tuning Manager earlier than 4.0 on a machine on which Device Manager 4.0 or later has been installed.
- When using another HiCommand Suite product, make sure that you back up the database for the relevant product.

- The HiCommand Device Manager server cannot coexist with the following HiRDB products. Therefore, do not install the HiCommand Device Manager server on a machine on which any of the following HiRDB products are installed. In addition, do not install these HiRDB products on a machine on which the HiCommand Device Manager server is installed.
 - HiRDB/Single Server
 - HiRDB/Parallel Server
 - HiRDB/Workgroup Server
 - HiRDB/Run Time
 - HiRDB/Developer's Kit
 - HiRDB SQL Executer

4.3.1.4 Checking Other Information

- You must log on as a root user.
- You must revise the Solaris or Linux OS parameters (kernel parameters and shell restrictions). To change the kernel parameters to the appropriate values, see section 4.12 for Solaris, or section 4.13 for Linux. If the kernel parameter setting is not correct, installation will fail.
- Verify that the following directories can be created, or that they have already been created and are write-enabled.
 - `/etc/init.d`
 - `/opt/HiCommand`
 - `/opt/hitachi`
 - `/var/opt/HiCommand`
 - `/var/opt/hitachi/HNTRLib2`
- Verify that symbolic links that have the following names have not been created. If they have been created, installation might fail.
 - `/opt`
 - `/var/opt`
 - `/var/tmp`
 - The names of the directories in `/opt/HiCommand` (including `/opt/HiCommand`)
 - The names of the directories in `/var/opt/HiCommand` (including `/var/opt/HiCommand`)
- Do not attempt a downgrade installation for Device Manager. For example, in an environment in which Device Manager 5.0 has been installed, you cannot install Device Manager 4.3 or an earlier version. However, a build to which patches have been applied can be overwritten by a build without the patches, as long as the version-revision numbers are the same.

- To use the service discovery feature in Solaris, the SLP daemon must be enabled before HiCommand Device Manager is installed (perform setup so that the SLP daemon starts automatically when the system starts). For information on how to enable the SLP daemon in Solaris, see section 11.5.1.2.
- In Linux, firewall exceptions must be registered manually before installation. For details on how to do this, see section 2.5.
- Do not specify the system's zone settings during installation in Solaris 10 system. If you do specify the settings, installation might finish abnormally.

4.3.2 Reviewing the Contents of the Installation CD

The Device Manager Server installation CD includes the following applications:

- Java 2 JRE software: version 1.4.2_06
- Device Manager Server software
- HiCommand Suite Common Component software
- HiRDB Database version 7.0

Once these products are installed, the Device Manager client software can be downloaded, installed and updated on the client systems from the Device Manager Server.

Installation requires root access, so you must be logged in as root to run the installation. You can use the **su** command to assume root privileges to run the installation.

4.4 Installing Device Manager Server and Common Component

After finishing a new installation, be sure to back up the HiCommand Device Manager server database.

To install Device Manager Server:

1. Log on to the Solaris(TM) or Linux system as the root user.
2. Stop any other HiCommand Suite software that is running.
3. Insert the HiCommand Device Manager CD-ROM. If the CD-ROM is not automatically mounted, mount the CD-ROM to `/mnt/cdrom`.
4. Move the current directory to the directory that stores the installer of Device Manager (`install.sh`). And then, execute the following command:

```
# ./install.sh
```

WARNING: Do not use **Ctrl + C** to stop in the middle of the installation. If you stop the installation, check the installation progress as follows:

- For Solaris:
Execute the `pkginfo HDVM` command.
- For Linux:
Execute the `rpm -qi HDVM` command.

If the Device Manager information is displayed, uninstall (see section 4.10.1 for instructions) and then re-install the Device Manager Server.

5. A message displays, asking whether the kernel parameter has been set up (see Figure 4.1). If the parameter has not been set up, select **n** to cancel the installation. If the parameter has been set up, select **y** to continue. For details about setup of the kernel parameters, see section 4.12 for Solaris, or see section 4.13 for Linux

Caution: If the kernel parameters are not set correctly, a message notifies you that the machine must be restarted after the kernel parameters are reset, and installation stops (see Figure 4.2). In Linux, the name of the OS parameter in which an error occurred is also displayed.

Caution: Figure 4.1 and Figure 4.2 show the output examples in Solaris. In Linux, `Kernel parameter` will be replaced with `os parameter`.

6. When the HiCommand Suite Common Component services are running, a message is displayed to confirm whether you want these services to stop. If you want to stop the installation, select **n**. If you want to continue the installation, select **y** (see Figure 4.3).

If the installer cannot stop the HiCommand Suite Common Component services, a message is displayed to notify you that you need to start the installation after stopping the other HiCommand Suite products, and then the installation stops (see Figure 4.4).

7. If HiCommand Suite Common Component is already installed, a message appears, recommending that you make a backup (see Figure 4.5). For more information about how to back up the database other HiCommand Suite products databases, see the relevant manual for each product. If you have not yet performed a backup, select **2** to cancel the installation. If a backup is not needed or has already been performed, select **1**.

8. In Solaris, the available HiCommand Device Manager packages are displayed. Press **Enter** to continue (see Figure 4.6). When the Common Component is being installed at version 4.0 or later, the HiRDB database will also be installed for database management functionality.
9. The license agreement displays. Select **y** to continue.
10. The SNMP Trap Note message displays (see Figure 4.7). Make sure that no other software products are using port 162 (if this is not the case, the error message in Figure 4.8 is displayed), and then press **Enter**.

If you want to disable the SNMP Trap reception function to start Device Manager, choose Yes to continue. If you want to change the settings of the product that is using port 162 and re-execute the installation, choose No to cancel the installation.

Caution: If you choose **y**, the properties for the SNMP Trap reception function are automatically changed to disable the function. You must reset these properties to the default values manually.
11. If the Common Component 4.0 or later has not already been installed, specify a directory for the Common Component database files (see Figure 4.9).

Caution: The file name has the following requirements:

 - The file name must be 90 bytes or fewer, and you must specify an absolute path to it.
 - Do not enter a path delimiter (/) at the end of the directory path.
 - You can use alphanumeric characters, underscores and periods for the path name
12. Specify a directory for the Device Manager Server database files. The server database file name has the same restrictions as the Common Component database file name (see Figure 4.10).
13. A message appears, prompting you to enter the IP address or host name of the target server, and the port number to be used (see Figure 4.11).

Important: The default port number is 23015, which will automatically be selected if you press **Enter** without changing the number. If you change the port number, you must also change that port number in the Common Component. For information on how to change a Common Component port number, see section 5.4.2.
14. A message about the settings for the SMI-S Provider service appears (Figure 4.12). If you want the SMI-S Provider service to start automatically when Device Manager starts, select **1** to continue. If you do not want it to start automatically, select **2** to continue.

If you selected **1**, set up the options by following the instructions in steps 15 through 18. If you selected **2**, go to step 19.

Note: You can set up the SMI-S Provider service after installation. For details, see Chapter 11.
15. A message about the SSL settings for SMI-S appears (see Figure 4.13). If you want to use SSL with SMI-S using the default port number (5989), select **1** to continue. If you want to use SSL with SMI-S, but you want to specify the port number yourself, select **2** to continue. If you want to use the default port number (5988) for SMI-S, but you do not want to use SSL, select **3** to continue. If you want to specify the port number for SMI-S by yourself, but do not want to use SSL, select **4** to continue.

Note: You can enable SSL and set the port number after installation. For details, see sections 11.3.2.2 and 11.4.1.

16. A message about changing the port number appears (see Figure 4.14). Enter the port number to be used, as required.
17. A message about two-way authentication for object operations and event indications appears (see Figure 4.15). If you do not want to use two-way authentication, select **1** to continue. If you want to use two-way authentication only for object operations, select **2** to continue. If you want to use two-way authentication only for event indications, select **3** to continue. If you want to use two-way authentication for both object operations and event indications, select **4** to continue.

Caution: Two-way authentication involves import and export of authentication files. For details, see section 7.4.

Note: You can enter settings to enable two-way authentication after installation. For details, see section 7.4.

18. A message about the settings for the SLP daemon appears (see Figure 4.16). To install and enable the SLP daemon, select **1** and then proceed to the next step. If you do not want to enable the SLP daemon, or if another SLP daemon is already installed and enabled, select **2** and then proceed to the next step.

Important: In Solaris, the SLP daemon must be enabled before HiCommand Device Manager is installed. Accordingly, select **2** here.

Note: In Linux, it is possible to enable the SLP daemon after installing HiCommand Device Manager. For details, see section 11.5.

19. The Device Manager package confirmation message is displayed (see Figure 4.17). Select **y** to start the installation. If the Common Component has not previously been installed at version 4.0 or higher, it will be installed during the Device Manager installation.
20. The **Secure Socket Certificates Note** panel displays (see Figure 4.18). Press **Enter** to continue.
21. A message displays indicating that the installation completed successfully and the Server and Common Component are starting. Be sure to refresh all registered subsystems at this point.

Note: If the installer ends with an error, follow the instructions on the error message and re-install Device Manager. Check the installation progress as follows.

- For Solaris:
Execute the `pkginfo HDVM` command.
- For Linux:
Execute the `rpm -qi HDVM` command.

If the Device Manager information is displayed, first uninstall and then reinstall Device Manager. See section 4.10 for instructions on uninstalling the Device Manager server.

Important: After installing the HiCommand Device Manager server, you need to register a license key by using Web Client. For information about how to register a license key, see the *HiCommand Device Manager Web Client User's Guide*.

```
WARNING: The kernel parameters must be set before installing HiCommand Device
Manager.
If the kernel parameters have already been set for another application, the
value for HiCommand Device Manager must be added to the existing settings.
If the kernel parameters have not been set, enter n to cancel installation.
If the kernel parameters have been set, enter y to continue installation.
Have the kernel parameters for HiCommand Device Manager been set? [y/n]
```

Figure 4.1 Message that Confirms the Setup of the Kernel Parameter

```
ERROR: The value of an effective kernel parameter doesn't fill the lower bound
value of Device Manager. Please check the settings of the kernel parameter and
reboot the system. The installation is stopped.
```

Figure 4.2 Error Message for the Setup of the Kernel Parameter

```
Stop HiCommand Suite Common Component Services:
To continue processing, HiCommand Suite Common Component services will be
stopped. However, these services cannot stop if a service of another HiCommand
Suite product is running. So, before continuing, please stop the services of
all other HiCommand Suite products.

Do you want to continue installation? [y/n]
```

Figure 4.3 Message that Confirms Stopping of Services (appears during installation)

```
ERROR: HiCommand Suite processes are running. Perform the following operation,
and redo the install process:
1. If applicable, stop other HiCommand Suite software except the Device
Manager.
2. Stop the Device Manager Server.
3. Stop HiCommand Suite Common Component. Execute the following command:
/opt/HiCommand/Base/bin/hcmdssrv -stop
```

Figure 4.4 Message Notifying that Another HiCommand Suite Product Is Running (appears during installation)

```
Backup recommendation:
If HiCommand Suite products have already been installed, it is strongly
recommended that you back up the HiCommand Suite Common Component database and
the databases for each installed HiCommand Suite product. What do you want to
do?
1. Continue the installation.
2. Stop the installation to manually perform backup.
Enter 1 or 2:
```

Figure 4.5 Backup Recommendation Reminder

```

Checking user.
Starting HiCommand Device Manager installation.
Checking OS and version.
Checking HiCommand Suite.
HiCommand Suite Common Component is not installed.
Checking HiCommand Device Manager process.
Now checking the HDvM version...
Checking HiCommand Device Manager installation.
Starting HiCommand Device Manager package Installation.
The following packages are available:
1 HDvM HiCommand Device Manager (Build 0550-xx)
(sparc) 5.5
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:

```

Figure 4.6 Available Packages for Installation

```

SNMP Trap Note:
HiCommand Device Manager uses UDP port 162 to listen for SNMP traps.
If another product uses port 162, after installation you need to disable
listening for SNMP traps by changing the property of HiCommand Device Manager.
Hit Enter Key to Continue.

```

Figure 4.7 SNMP Trap Note

```

Setting for the SNMP Trap Reception Function:
Another application is using the port used to listen for SNMP traps.
To use Device Manager, you must disable the SNMP trap reception function of
Device Manager.
Do you want to disable the SNMP trap reception function of Device Manager?
Do you want to continue installation? (Y/N):

```

Figure 4.8 Settings for the SNMP Trap Reception Function

```

Specify the storage destination for the database files that HiCommand Suite
Common Component will use.
Note: At least 1.2 GB of free space is required.
[default=/var/opt/HiCommand/Base/database]

```

Figure 4.9 Specifying Common Component Database Files

```

Specify the storage destination for the database file that HiCommand Device
Manager will use.
Note 1: At least 100 MB of free space is required.
Note 2: For an upgrade installation, at least 100 MB or four times the file
size of HiCommand.gdb (whichever is the largest) is required.
[default=/opt/HiCommand/HiCommandServer/database]

```

Figure 4.10 Specifying HiCommand Device Manager Database Files

```

Enter the IP address or host name of the server that the client accesses from
a Web browser:
> **.*.*.*.*
Enter the port number of the server that the client accesses from a Web
browser [default=23015]:
>
The port number 23015 is selected.

```

Figure 4.11 Entering IP address and Port Number

```
Setting for the SMI-S Provider Service:
Do you want the CIM/WBEM function to be enabled automatically after
installation?
(The CIM/WBEM function is only necessary if you need to access Device Manager
by using an SMI-S client.)

1. YES. Automatically enable the function after installation.
2. No.
Enter 1 or 2 [default=2]:
```

Figure 4.12 Settings for the SMI-S Provider Service

```
Setting for the SMI-S SSL:
Do you want to use SSL for SMI-S operations?
1. YES. (Default port number is 5989.)
2. YES. (I will change the port number.)
3. NO. (Default port number is 5988.)
4. NO. (I will change the port number.)
Enter 1, 2, 3 or 4. [default=1]:
```

Figure 4.13 SSL Settings for SMI-S

```
Change the port number if needed.
Enter the port number:
```

Figure 4.14 Changing the Port Number

```
Do you want to also use Two-way Authentication for the following operations?
1. NO.
2. Also use Two-way Authentication for Object operations.
3. Also use Two-way Authentication for Event Indications.
4. Also use Two-way Authentication for both Object operations and Event
Indications.
Enter 1, 2, 3 or 4. [default=3]:
```

Figure 4.15 Two-way Authentication for Object Operations and Event Indications

```
Setting for the SLP Daemon:
Do you want the SLP function to be enabled automatically after installation?
(The SLP function is required from SMI-S client. If you have not installed
other SLP daemon, you need to install our SLP daemon.)

1.YES. Automatically enable the function after installation.
2.NO.
Enter 1 or 2 [default=1]:
```

Figure 4.16 Setting the SLP Daemon


```

URL Information. [Host name: 10.60.71.15, Port number: 23015]
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.
This package contains scripts which will be executed with super-user
permission during the process of installing this package.
Do you want to continue with the installation of <HDVM> [y,n,?] y

```

Figure 4.17 Installing Device Manager

```

Secure Socket Certificates Note:
If secure socket communications (https://) with HiCommand Device Manager are
expected, it is necessary to generate Certificate to the following two
servers.

1) HiCommand Device Manager Server
2) HBase Storage Mgmt Web Service
Hit Enter Key to Continue.

```

Figure 4.18 Secure Socket Certificates Note

4.4.1 Upgrading or Re-installing Device Manager

After finishing an upgrade installation, be sure to back up the HiCommand Device Manager Server database.

4.4.1.1 General Considerations for Upgrade and Re-installation

Device Manager will be installed in:

/opt/HiCommand

The Common Component will be installed in:

/opt/HiCommand/Base

Important: The characters that can be used for user IDs in HiCommand Device Manager server (version 3.5 or later) are as follows:

A-Z a-z 0-9 - _ . @ + #.

Important: The characters that can be used for passwords in version 03-01-/A are as follows:

A-Z a-z 0-9 ! # \$ % & () * + - . = @ \ ^ _ | ' .

If you have user IDs or passwords with unusable characters, you need to re-register those users.

If all of the System Administrators have user IDs or passwords with unusable characters, create a new System Administrator user ID, as follows:

1. Back up the current server database. See section 3.7.1 for instructions.
2. Uninstall the Device Manager Server (version 3.5 or later). See section 4.10.1 for instructions.
3. Install the Device Manager Server at version 2.4 or earlier.
4. Restore the database. See section 4.8.2 for instructions.
5. Create a new user by using the appropriate characters for user IDs and passwords.
6. Re-install the Device Manager Server at version 3.5 or later.
7. Clear the cache in Java Web Start.

CAUTION: Wait several minutes after the upgrade or re-installation finishes before stopping the service, because the database must be updated with the latest information.

WARNING: Do not cancel in the middle of an upgrade or re-installation, because doing so could corrupt the files.

If you are updating the Common Component database and an error occurs and auto-recovery fails, you must manually recover the database before you re-install the server. Once you upgrade or re-install the server, you will not be able to recover the Common Component database. To find a database update error, check the following log file:

<installation directory>/Base/log/hcmdsdbupdate.log. You will want to restore the file named **<installation directory>/Base/database/hbase_vup_back.gbk.**

If you install a new version of the Device Manager server, the new version overwrites the existing version. Device Manager automatically updates your data and configurations to work with the latest version. The previous **HiCommandCLI.properties** file is saved as **HiCommandCLI.properties.old** in the same directory. The previous **TIA.properties** file is saved as **TIA.properties.old** in the same directory.

Important: If the **HiCommandCLI.properties** file contains multiple entries of the same key with different values, the value of the most recently specified key overrides the others. Although key duplication does not affect HiCommand CLI operations, we do not recommend that you specify the same key more than once with different values. Instead, eliminate unnecessary duplicate keys and their values. If there are duplicate keys that have different values during an upgrade installation, the new **HiCommandCLI.properties** file will inherit keys as follows:

If there are multiple **password** keys:

All **password** keys and their values in the old **HiCommandCLI.properties** file are written to the new file as is. The following shows an example:

- The **password** keys and their values in the old file:
`password=AAA`
`password=BBB`
- The **password** keys and their values written to the new file:
`password=AAA`

```
password=BBB
```

If there are duplicate keys other than `password`:

The name and value of the most recent duplicate key in the old `HiCommandCLI.properties` file are written to the new file as many times as there are duplicated keys. The following shows an example:

- The `user` keys and their values in the old file:

```
user=AAA
```

```
user=BBB
```

- The `user` keys and their values written to the new file:

```
user=BBB
```

```
user=BBB
```

WARNING: If either InterBase or InterServer have previously been installed, that service must be running when you upgrade the Device Manager Server.

WARNING: If you have made any changes to `/opt/HiCommand/Base/conf/init.conf`, and you are upgrading from Device Manager version 3.0 or 3.1 to version 3.5 or later, you must first create a new folder for `/opt/HiCommand/Base/conf/user.conf`, and duplicate those changes in this file.

Note: User-created files will not be saved as `*.old` during the upgrade.

4.4.1.2 When Upgrading From Versions 2.2 Through 3.5 to Version 4.0 or Higher

You cannot upgrade directly from Device Manager version 2.2 to version 4.0 or higher. You must first upgrade to a version between 2.3 and 3.5, and then upgrade to version 4.0 or higher.

Caution: If either InterBase or InterServer has previously been installed, that service must be running when you upgrade the Device Manager Server.

Caution: If version 2.2 or earlier of the HiCommand Device Manager server has been installed, the users `hicmd` and `interbase`, and the user group `hicmd` have been created. If the package was installed more than once, users `hicom0` to `hicom999` and user groups `interb0` to `interb99` might have been created. Version 2.3 or later of the HiCommand Device Manager server does not use these users. If these users are not necessary, delete them manually.

Caution: When version 1.1 or earlier of the HiCommand Device Manager server is installed and an overwrite installation is performed, every volume in each logical group is displayed as a CVS volume. Also, disk usage information is not displayed. To avoid this problem, refresh all storage subsystems which were discovered by version 1.1 or earlier of the HiCommand Device Manager server.

Note: If the older version of HiCommand Device Manager was not installed in `/opt/HiCommand/`, the upgrade of HiCommand Device Manager will not execute properly. If this is the case:

- Back up old files manually.
- Uninstall the older version of the HiCommand Device Manager server.
- Move the current directory to the root (/), and then execute the following command:

```
# installation-directory-for-the-Device-Manager-server/Uninstall/uninstall.sh
```

- Perform a new installation to install the new version of the HiCommand Device Manager server.

4.4.1.3 About User Information in Version 5.0 and Higher

In version 5.0 or higher, user information is managed by using the user management functionality of HiCommand Suite Common Component. The registered user information is migrated to the HiCommand Suite Common Component repository when the Device Manager server is started for the first time after the upgrade installation. For this migration, also note the following points:

- If there is user information that cannot be migrated to the HiCommand Suite Common Component repository due to data corruption or another problem, that information is output to the Device Manager trace log file.
- If user accounts with the same user ID but different passwords have been registered in both HiCommand Suite Common Component and Device Manager, the user account in HiCommand Suite Common Component overrides the one in Device Manager. The user account registered in Device Manager becomes unavailable, and information to that effect is output to the Device Manager trace log file.
- If user accounts that have the same user ID and password have been registered in both HiCommand Suite Common Component and Device Manager, the user account in Device Manager is added to the one in HiCommand Suite Common Component.
- You cannot migrate the user account whose user ID is `System`. The user management functionality of HiCommand Suite Common Component defines this user ID as having the `Admin` permission for all HiCommand Suite products (version 5.0 or later).

4.4.2 Performing an Upgrade Installation from Version 3.5 or Earlier

To upgrade the HiCommand Device Manager Server:

1. Log on to the Solaris system as the root user.
2. If any other HiCommand Suite software is running, stop that process.
3. Insert the HiCommand Device Manager CD-ROM. If the CD-ROM is not automatically mounted, mount the CD-ROM to `/mnt/cdrom`.
4. Move the current directory to the directory that stores the installer of Device Manager (`install.sh`). And then, execute the following command:

```
# ./install.sh
```

WARNING: Do not use **Ctrl + C** to stop in the middle of the installation. If you stop the installation, check the installation progress as follows:

Execute the `pkginfo HDVM` command.

5. A message displays, asking whether the kernel parameters have been set up (see Figure 4.1). If the parameters have not been set up, select **n** to cancel the installation; otherwise, select **y** to continue.

Caution: If the kernel parameters are not set correctly, a message notifies you that the machine must be restarted after the kernel parameters are reset, and installation stops (see Figure 4.2).

6. When the HiCommand Suite Common Component services are running, a message is displayed to confirm whether you want these services to stop. If you want to stop the installation, select **n**. If you want to continue the installation, select **y** (see Figure 4.3).

If the installer cannot stop the HiCommand Suite Common Component services, a message is displayed to notify you that you need to start the installation after stopping the other HiCommand Suite products, and then the installation stops (see Figure 4.4).

7. If InterBase has not been installed (see Figure 4.19), or if the InterBase version is not 6.0 (see Figure 4.20), an upgrade installation cannot be performed without InterBase 6.0 installed.

If InterBase 6.0 has not been installed, uninstall the HiCommand Device Manager server and then start a new installation, or install HiCommand Device Manager 3.5 or earlier and then perform an upgrade installation.

If the version of InterBase is incorrect, an upgrade installation cannot be performed. In this case, uninstall the HiCommand Device Manager server, and then start a new installation.

8. If InterClient has not been installed (see Figure 4.21), or the version of InterClient is not 2.0 (see Figure 4.22), an upgrade installation cannot be performed without InterClient 2.0 installed.

If InterClient 2.0 has not been installed, uninstall the HiCommand Device Manager server and then start a new installation, or install HiCommand Device Manager 3.5 or earlier and then perform an upgrade installation.

If the version of InterClient is incorrect, an upgrade installation cannot be performed. In this case, uninstall the HiCommand Device Manager server, and then start a new installation.

9. Device Manager is displayed as an available package. Press **Enter** to continue.

You cannot downgrade Device Manager. If you attempt to do so, an error message (Figure 4.23) displays and installation stops. However, if the version and revision numbers of the builds before and after a selected package are the same, and the selected package has an earlier (outdated) service pack, the HiCommand Device Manager downgrade message appears (Figure 4.24). In that case, select **y** to continue.

10. The license agreement displays. Select **y** to continue.

11. If the Common Component 4.0 or later has not already been installed, specify a directory for the Common Component database files.

Caution: The file name has the following requirements:

- The file name must be 90 bytes or fewer, and you must specify an absolute path to it.
- Do not enter a path delimiter (/) at the end of the directory path.
- You can use alphanumeric characters and spaces for the path name

12. Specify a directory for the Device Manager Server database files. The server database file name has the same restrictions as the Common Component database file name (see Figure 4.9).

13. If HiCommand Suite Common Component 3.0 or later has not been installed, a message appears, prompting you to enter the IP address or host name of the installation-target server, and the port number to be used (see Figure 4.11).

Important: If you press the **Enter** key without entering anything, the default port 23015 is specified. When changing the port, you must also change the port in HiCommand Suite Common Component. For details on how to change the HiCommand Suite Common Component port, see section 5.4.2.

14. The HiCommand Device Manager package confirmation message is displayed. Select **y** to start the installation. If HiCommand Suite Common Component has not been installed, it is installed during the installation of HiCommand Device Manager.

15. If you are upgrading from Device Manager version 3.5 or lower to version 4.0 or higher, the Database conversion message displays (see Figure 4.26):

If you select **1**, the installer automatically converts the database. If the database conversion fails, an error message displays (see Figure 4.26). A confirmation message will display when the conversion is finished, asking if you want to continue (see Figure 4.27). Select **Enter**.

Important: If an error occurs during the database conversion, you may need to take corrective action. For more information, see Chapter 10.

Note: It may take a long time to convert the database. For example, if 8,000 LDEVs and 16,000 paths have been managed, the database conversion will take about 10 minutes in an environment that has a 900 MHz CPU and 2 GB of memory.

If you select **2**, the installer will not convert the database. Convert the database manually after the installation finishes. For more information, see section 4.9.

16. When the database conversion finishes, a confirmation message is displayed, asking whether you want to continue installation. Press the Enter key to continue.

17. The Secure Socket Certificates Note panel displays (see Figure 4.18). Press **Enter** to continue.

18. A message displays indicating that the installation completed successfully and the Server and Common Component are starting. Be sure to refresh all registered subsystems at this point.

Note: If the installer ends with an error, follow the instructions on the error message and re-install Device Manager. Check the installation progress as follows.

- For Solaris:
Execute the `pkginfo HDVM` command.

- For Linux:

Execute the `rpm -qi HDVM` command.

If the Device Manager information is displayed, first uninstall and then reinstall Device Manager. See section 4.10 for instructions on uninstalling the Device Manager server.

```
ERROR:InterBase is required for an upgrade installation of HiCommand Device
Manager.
For a new installation, uninstall any installed HiCommand Device Manager, and
then install the new HiCommand Device Manager.For an upgrade installation,
install HiCommand Device Manager version 3.5 or earlier, and then install the
current version of HiCommand Device Manager.
```

Figure 4.19 When InterBase is Not Installed

```
ERROR: InterBase version is incorrect. An upgrade installation cannot be
performed because the operating environment of HiCommand Device Manager is
incorrect. Uninstall HiCommand Device Manager, and then perform the
installation.
```

Figure 4.20 Incorrect InterBase Version

```
ERROR:InterClient is required for an upgrade installation of HiCommand Device
Manager.
For a new installation, uninstall any installed HiCommand Device Manager, and
then install the new HiCommand Device Manager.
For an upgrade installation, install HiCommand Device Manager version 3.5 or
earlier, and then install the current version of HiCommand Device Manager.
```

Figure 4.21 InterClient Not Installed

```
ERROR: InterClient version is incorrect. An upgrade installation cannot be
performed because the operating environment of HiCommand Device Manager is
incorrect. Uninstall HiCommand Device Manager, and then perform the
installation.
```

Figure 4.22 Incorrect InterClient Version

```
ERROR: A newer version of HiCommand Device Manager is already installed on
this system.
You cannot downgrade HiCommand Device Manager.
For example:
1. If 5.0.0(5.0.0-xx) is already installed, you cannot install 4.2.0(4.2.0-xx)
in an update installation.
2. If 4.3.0(4.3.0-xx) is already installed, you cannot install 4.2.0(4.2.0-xx)
in an update installation.
```

Figure 4.23 Upgrade Error Message

```
WARNING: A newer version of HiCommand Device Manager is already installed on
this system.
If you continue installation, you will downgrade HiCommand Device Manager.
For example:
1. If 5.0.0(5.0.0-xx) is already installed, you cannot install 4.2.0(4.2.0-xx)
in an update installation.
2. If 4.3.0(4.3.0-xx) is already installed, you cannot install 4.2.0(4.2.0-xx)
in an update installation.

Do you want to continue installation? (Y/N):
```

Figure 4.24 Downgrade Error Message

```
Database Conversion:
To use the new version of HiCommand Device Manager, the database currently
being used must be converted. Database conversion might take a long time.
Select the data conversion method from the following:
1. Convert the database during installation.
2. Convert the database after installation finishes, by using the database
conversion command.
To convert the database during installation, enter [1].
To convert the database after installation, enter [2].
```

Figure 4.25 Database Conversion Message

```
ERROR: An attempt to convert the database has failed.
After installation but before starting HiCommand Device Manager, execute the
database conversion command.
Note: Even if a reinstallation is performed, database conversion is not
performed.
Use the database conversion command to perform database conversion.
```

Figure 4.26 Data Update Error Message

```
...
Service startup finished:
Startup of the service has finished.
After installation finishes, refresh all registered subsystems.
Hit Enter Key to Continue.
```

Figure 4.27 Database Conversion Confirmation Message

4.4.3 Performing an Upgrade Installation from Version 4.0 or Later or a Re-installation

After finishing an upgrade installation or re-installation, be sure to back up the HiCommand Device Manager server database.

Warning: Do not cancel in the middle of an upgrade installation or re-installation, as doing so could corrupt the files.

Note: Files created by a user will not be saved as *.old during the upgrade installation or re-installation.

To manually make a backup before performing an upgrade installation or re-installation of the Device Manager server, copy the following files and directories to another location:

- `/opt/HiCommand/HiCommandServer/config/*.properties`
The old `/*.properties` files are backed up in the `config` directory as `/*.properties.old`. Note, however, that files created by a user will not be backed up.
- `/opt/HiCommand/HiCommandServer/logs`
To back up the log files, copy this directory to another location
- `/opt/HiCommand/HiCommandCLI/HiCommandCLI.properties`
The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same directory.
- `/opt/HiCommand/HiCommandCLI/legacy/R2.0/HiCommandCLI.properties`
The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same directory.
- `/opt/HiCommand/HiCommandCLI/legacy/R2.1/HiCommandCLI.properties`
The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same directory.
- `/opt/HiCommand/SupportTools/CollectTool/TIA.properties`
The old `TIA.properties` files are backed up as `TIA.properties.old` in the same directory.

The database can automatically be backed up or exported during installation. If you want to manually back up or export the database, perform the operations specified in sections 4.8.1 or 4.8.3.1. Decide whether to back up or export the database by referring to the following points.

- If version 5.1 or earlier of a HiCommand Suite product is already installed, back up the database. You cannot export the database.
- If version 5.5 or later of a HiCommand Suite product has already been installed and you will perform an upgrade installation, we recommend you export the database.
- If you will perform a re-installation, we recommend you back up the database.

To perform an upgrade installation or re-installation of the HiCommand Device Manager server:

1. Log onto the Solaris system as **root**.
2. If any other HiCommand Suite software is running, stop that process.
3. Insert the HiCommand Device Manager CD-ROM. If the CD-ROM is not automatically mounted, mount the CD-ROM to `/mnt/cdrom`.
4. Move the current directory to the directory that stores the installer of Device Manager (`install.sh`). And then, execute the following command:

```
# ./install.sh
```

WARNING: Do not use **Ctrl + C** to stop in the middle of the installation. If you stop the installation, run the **#pkginfo HDVM** command. If the Device Manager information is displayed, uninstall and then re-install the Device Manager Server.

5. A message appears, asking whether the kernel parameters have been set up (see Figure 4.1). If the parameters have not been set up, select **n** to cancel the installation. If the parameters have been set up, select **y** to continue. For details about setup of the kernel parameters, see section 4.12 for Solaris, or see section 4.13 for Linux.

Caution: If the kernel parameters are not set correctly, a message notifies you that the machine must be restarted after the kernel parameters are reset, and installation stops (see Figure 4.2). In Linux, the name of the OS parameter in which an error occurred is also displayed.

Caution: Figure 4.1 and Figure 4.2 show the output examples in Solaris. In Linux, `Kernel parameter` will be replaced with `OS parameter`.

6. When the HiCommand Suite Common Component services are running, a message is displayed to confirm whether you want these services to stop. To stop the installation, select **n**. To continue the installation, select **y** (see Figure 4.3).

If the installer cannot stop the HiCommand Suite Common Component services, a message is displayed to notify you that you need to start the installation after stopping the other HiCommand Suite products, and then the installation stops (see Figure 4.4).

7. A message asking whether you want to back up the database (see Figure 4.28) or export the database (see Figure 4.29) is displayed. If you want to back up or export the database, select **y** to start the backup or export. If you do not want to back up or export, select **n** to continue.

This operation backs up or exports all HiCommand Suite product databases. The following table describes the conditions whether the backup or export is performed, the backup-data storage destination directory, and the disk space required for the directory.

Table 4.7 Storage Destination of Backed up and Exported Data and Required Disk Space

Operation	Performing conditions	Data storage destination directory	Required disk space
Backup	▪ When the version of HiCommand Suite Common Component is 5.1 or earlier ▪ When the version of HiCommand Suite Common Component is 5.5 or later, and performing a re-installation of the same version and revision of HiCommand Device Manager	<code>/var/opt/HiCommand/olddbbackup_hdb</code>	See section 4.8.1.
Export	When the conditions for backing up data are not satisfied	<code>/var/opt/HiCommand/olddbexported_hdb</code>	See section 4.8.3.4.

Caution: Before backing up or exporting, the contents of the data storage destination directory are deleted (Figure 4.30 and Figure 4.31 show examples of the deletion confirmation panels displayed before backing up or exporting). If you want to save the old data, you need to copy it to another location beforehand, and then select **y** in the confirmation message.

Caution Backing up or exporting can fail due to insufficient disk space, or for other reasons. If this occurs, back up or export the databases manually. Then, select **n** to continue installation. For instructions on how to back up and restore the database, see section 4.8. For details about how to export a database, see section 4.8.3.

8. Device Manager is displayed as an available package. Press **Enter** to continue (see Figure 4.6). When the Common Component is being installed at version 4.0 or later, HiRDB will also be installed to manage the database.

You cannot downgrade Device Manager. If you attempt to do so, an error message will display (see Figure 4.23). However, if the version and revision numbers of the builds before and after a downgrade are the same, the HiCommand Device Manager downgrade message appears.

9. The license agreement displays. Select **y** to continue.
10. The SNMP Trap message displays (see Figure 4.7). Verify that you have no other software products using port 162, then press **Enter**.
11. A message appears, prompting you to enter the IP address or host name of the target server, and the port number to be used (see Figure 4.10).

Important: The default port number is **23015**, which will automatically be selected if you press Enter without changing the number. If you change the port number, you must also change that port number in the Common Component. For information on how to change a Common Component port number, see section 5.4.2.

12. The Device Manager package confirmation message is displayed (see Figure 4.17). Select **y** to start the installation.
13. The Secure Socket Certificates Note panel (see Figure 4.18) displays. Press **Enter** to continue.
14. A message displays indicating that the installation completed successfully.
If the system is in a cluster configuration, go to step 21.

15. Stop the Device Manager server and HiCommand Suite Common Component.
Execute the following command:

```
# /opt/HiCommand/suitesrvctl -stop_all
```

16. Edit the `pdsys` file and the `def_pdsys` file.

Change the value for the `pdunit` parameter's `-x` option to the loopback address `127.0.0.1`.

The default installation locations of the `pdsys` file and `def_pdsys` file are as follows:

```
/opt/HiCommand/Base/HDB/conf/pdsys
```

```
/opt/HiCommand/Base/database/work/def_pdsys
```

17. Edit the `pdutysys` file and the `def_pdutysys` file.

Change the value for the `pd_hostname` parameter to the loopback address `127.0.0.1`. If `pd_hostname` does not exist, add the `pd_hostname` parameter to set the loopback address.

The default installation locations of the `pdutssys` file and `def_pdutssys` file are as follows:

```
/opt/HiCommand/Base/HDB/conf/pdutssys
/opt/HiCommand/Base/database/work/def_pdutssys
```

18. Edit the `HiRDB.ini` file.

Change the value for the `PDHOST` parameter to the loopback address `127.0.0.1`.

The default installation location of the `HiRDB.ini` file is as follows:

```
/opt/HiCommand/Base/HDB/conf/emb/HiRDB.ini
```

19. Restart the machine.

20. Execute the following command to make sure that the HiCommand Suite Common Component service is running.

```
/opt/HiCommand/Base/bin/hcmdssrv -status
```

21. Refresh all the registered subsystems to update the database.

Note: If the installer ends with an error, follow the instructions on the error message and re-install HiCommand Device Manager. If the **pkginfo HDVM** command displays the package information, first uninstall and then re-install HiCommand Device Manager.

```
Device Manager will back up the database to the following directory during
installation:
/var/opt/HiComamnd/olddbbackup_hdb
Do you want to backup the database now? [y/n]
```

Figure 4.28 Selection Message for Backing Up the Database

```
Device Manager will export the database to the following directory during
installation:
/var/opt/HiComamnd/olddbexported_hdb
It takes time to export. Do you want to export the database now? [y/n]
```

Figure 4.29 Selection Message for Exporting the Database

```
Installer will backup the database to /var/opt/HiCommand/olddbbackup_hdb.
If this file exists, it will be replaced with a new backup file.
Do you want to continue? [y/n]
```

Figure 4.30 Backup Directory Deletion Confirmation Message

```
Before exporting the database, the following directory will be erased:
/var/opt/HiCommand/olddbexported_hdb.
Do you want to continue? [y/n]
```

Figure 4.31 Export Directory Deletion Confirmation Message

4.5 Installing Device Manager in a Cluster Server Environment

Caution: HiCommand Device Manager Server only supports Solaris cluster environments.

The HiCommand Device Manager server can provide higher availability in a cluster environment. This section discusses the requirements and settings for a supported cluster environment.

For information on how to change the cluster configuration to a non-cluster configuration after you have already started Device Manager Server operations, see section 4.5.6.

Important: If you are installing Device Manager in an environment where other HiCommand products are running in a cluster configuration, see section 4.5.2 for instructions.

4.5.1 System Requirements

The requirements for a cluster environment are as follows:

- Platform: Solaris 9 (32-bit or 64-bit kernel mode)
- Cluster software: VERITAS Cluster Server 3.5 or Sun Cluster 3.1
- Number of nodes: 2
- Cluster configuration: Active-standby configuration

Caution: During installation, there is a step to back up and migrate the databases. Make sure that you secure the free disk space for backup and migration before installation. For the disk space required to back up, see section 4.8.1. The target disk (that is placed on the shared disk or local disk) to which the database is to be migrated must have the same free disk space or more as the database of the migration source.

4.5.2 Setup Where Other HiCommand Products Are Installed

Follow these instructions when you have other HiCommand Suite products installed in a cluster configuration.

WARNING: In this procedure, the cluster configuration for other HiCommand Suite products is temporarily cancelled.

Important: When you execute this command, it will change the port used by HiRDB to its default (23032). If you are using a port other than the default, you must change it back.

1. Remove the services for all other HiCommand Suite products and the HiRDB service from the cluster monitoring target.
2. If you are using VERITAS Cluster Server:
 - Start Cluster Manager on the Java Console.
 - For each HiCommand Suite service, do the following:
Place the service offline by right-clicking the service and then clearing **Enabled** from the menu.

In the Cluster Explorer window, select the **Service Groups** tab, then select the group in which the HiCommand Suite product service has been registered.

Right-click the service, and select **Freeze** and then **Temporary**.

3. If you are using Sun Cluster Server:

- Disable the resource monitoring for each HiCommand Suite product service:

```
# /usr/cluster/bin/scswitch -n -M -j resource-name
```

- Disable the resources for each HiCommand Suite product service:

```
# /usr/cluster/bin/scswitch -n -j resource-name
```

4. Stop all HiCommand Suite products in both the executing and standby nodes. See the manuals for the individual products if you need instructions.

5. Stop the Common Component in both the executing and standby nodes:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

6. If you are using VERITAS Cluster Server, switch each group where a HiCommand Suite product service has been registered into the standby system, as follows:

- In the Cluster Explorer window, select the **Service Groups** tab.
- For each group in which the HiCommand Suite product service has been registered, do the following:

Right-click the group, then select **Unfreeze** from the pop-up menu.

Right-click the group, then select **Switch To** and then **Host Name** from the pop-up menu.

Right-click the group. Select **Freeze** and then **Temporary** from the pop-up menu.

7. If you are using Sun Cluster, switch each group where a HiCommand Suite product service has been registered into the standby system, as follows:

```
# /usr/cluster/bin/scswitch -z -g group-name -h host-name
```

8. On the standby node:

- Delete or empty the data input/output target directory.
- Start HiRDB:

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

- Back up the database (see section 4.8.1 if you need instructions).
- In the standby node, migrate the database to your local disk.

Delete or empty **target-directory-for-storing-data**, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -removecluster -databasepath
target-directory-for-recreating-database -exportpath target-directory-for-storing-
data
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -removecluster -databasepath
/root/re_creating_db -exportpath /opt/storing_data
```

Caution: Specify an absolute path (63 bytes maximum) for *target-directory-for-recreating-database* and *target-directory-for-storing-data*.

Caution: *target-directory-for-recreating-database* and *target-directory-for-storing-data* must be placed on your local disk.

Caution: The characters that can be used for *target-directory-for-recreating-database* and *target-directory-for-storing-data* are as follows. In addition to these characters, a forward slash (/) can be used as a path delimiter. You cannot use a space in a path.

A-Z a-z 0-9 . _

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

9. Switch each group in which the HiCommand Suite product service has been registered into the executing system.

10. On the executing node:

- Empty the **<data input/output target directory>**
- Start HiRDB on the executing node:

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

- Back up the database (see section 4.8.1 if you need instructions).
- In the executing node, migrate the database to your local disk.

Delete or empty **target-directory-for-storing-data**, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -removecluster -databasepath
target-directory-for-recreating-database -exportpath target-directory-for-storing-
data
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -removecluster -databasepath
/root/re_creating_db -exportpath /opt/storing_data
```

Caution: Specify an absolute path (63 bytes maximum) for *target-directory-for-recreating-database* and *target-directory-for-storing-data*.

Caution: *target-directory-for-recreating-database* and *target-directory-for-storing-data* must be placed on your local disk.

Caution: The characters that can be used for *target-directory-for-recreating-database* and *target-directory-for-storing-data* are as follows. In addition to these characters, a path delimiter (/) can be used. You cannot use a space in a path.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

11. Install HiCommand Device Manager server and configure a cluster environment by referring to section 4.5.3.

For information on how to set up a cluster environment for other HiCommand Suite products, see the relevant manual for each product.

4.5.3 Performing a New Device Manager Installation

After finishing a new installation, be sure to back up the Device Manager server database.

Before installing Device Manager, make sure that the cluster management IP address and shared disk are enabled on the executing node.

4.5.3.1 Installing and Configuring the Executing Node

Caution: While performing cluster configuration, do not access HiCommand Device Manager.

1. If the service of another HiCommand Suite product or cluster group exists, exclude it from cluster management.
2. Install Device Manager on the executing node (see section 4.4 if you need instructions). Note the following requirements:
 - Leave the settings specifying the location of the databases for the Common Component and the Device Manager Server as the default values.
 - For the IP address of the Device Manager Server, specify a logical host name.

Important: A logical host name indicates the name of a virtual host allocated to the cluster management IP address, which must be enabled and accessible.

3. After the Device Manager Server is installed on the executing node, use the Web Client to enter the license key. For further information on the Device Manager Web Client, please see the *HiCommand Device Manager Web Client User's Guide*.

Note: You should have received a CD that contains the HiCommand Device Manager License Key. Upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found simply highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.

4. Use a text editor to create a cluster configuration file, and specify the following items:
 - mode: online for the executing node, and standby for the standby node.
 - virtualhost: the logical host name.
 - onlinehost: the executing node host name.
 - standbyhost: the standby node host name.

The following shows a coding example in the cluster-configuration file:


```

mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2

```

5. Save the created file as **cluster.conf** in /opt/HiCommand/Base/conf.

Caution: An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`. Make sure that the IP address can be resolved from the host name. An IP address that is enabled and accessible must be assigned to the logical host name to be specified in `virtualhost`.

6. Stop the Device Manager Server and the Common Component using the following command:

```
# /opt/HiCommand/suitesrvctl -stop_all
```

7. Start HiRDB by executing the following command:

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

8. Back up the database (see section 4.8.1 for instructions).

9. Migrate the database to the shared disk.

Delete or empty *target-directory-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -cluster -databasepath target-
directory-for-recreating-database -exportpath target-directory-for-storing-data
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath
/root/re_creating_db -exportpath /opt/storing_data
```

Caution: Specify an absolute path (63 bytes maximum) for **target-directory-for-recreating-database** and *target-directory-for-storing-data*.

Caution: *target-directory-for-recreating-database* must be placed on a shared disk. *target-directory-for-storing-data* must be placed on your local disk.

Caution: The characters that can be used for *target-directory-for-recreating-database* and *target-directory-for-storing-data* are as follows. In addition to these characters, a forward slash (/) can be used as a path delimiter. You cannot use a space in a path.

A-Z	a-z	0-9	.	_
-----	-----	-----	---	---

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

10. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

11. Set the Common Component so that it does not start automatically when the machine starts:

/opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

12. Set the Device Manager server so that it does not start automatically when the machine starts, either by moving the following file to another directory, or by changing its file name.

Important: the new file name should not begin with either k or s:

/etc/rc3.d/S99hicommand

4.5.3.2 Installing and Configuring on the Standby Node

1. Install Device Manager on the executing node (see section 4.4 if you need instructions). Note the following requirements:
 - Leave the settings specifying the location of the databases for the Common Component and the Device Manager Server as the default values.
 - For the IP address of the Device Manager Server, specify a logical host name. A logical host name indicates the name of a virtual host allocated to the cluster management IP address, which must be enabled and accessible.

2. After the Device Manager Server is installed on the standby node, use the Web Client to enter the license key.

Note: You should have received a CD that contains the HiCommand Device Manager License Key. Upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found, highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.

3. Use the IP address of the standby node to access the Device Manager Server.
4. Use a text editor to create a cluster configuration file, and specify the following items:
 - **mode:** online for the executing node, and standby for the standby node.
 - **virtualhost:** the logical host name.
 - **onlinehost:** the executing node host name.
 - **standbyhost:** the standby node host name.

5. Save the created file as **cluster.conf** in **/opt/HiCommand/Base/conf**.

Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

6. Stop the Device Manager Server and the Common Component using the following command:

/opt/HiCommand/suitesrvctl -stop_all

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

7. Set the database system on the shared disk as the one to be referenced. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

/opt/HiCommand/Base/bin/hcmdsdbremake -cluster -databasepath target-directory-for-recreating-database>

The following shows an example of executing the command:

/opt/HiCommand/Base/bin/hcmdsdbremake -cluster -databasepath /root/re_creating_db

Note: Specify the same directory as the directory specified for *target-directory-for-recreating-database* on the executing node. Do not specify a path that includes a space.

Note: For details about how to set the port that HiRDB uses, see section 5.4.2.

Deploy the directory in which the database is to be re-created on the shared disk.

8. If HiCommand Suite Common Component is running, execute the following command to stop it.

/opt/HiCommand/Base/bin/hcmdssrv -stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

9. Perform setup so that the Common Component service does not start automatically when the machine starts, using the following command:

/opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

10. Set the Device Manager server so that it does not start automatically when the machine starts, either by moving the following file to another directory, or by changing its file name.

/etc/rc3.d/S99hicommand.

Important: the new file name should not begin with either k or s.

4.5.3.3 Creating Scripts for VERITAS Cluster Server

Note: If you are using Sun Cluster Server, skip this section and go to section 4.5.3.4.

1. After installing and setting up HiCommand Device Manager on the executing node and standby node, you must create the script for HiRDB on both nodes.
2. Create the dummy file for monitoring the HiRDB service from VERITAS Cluster Server.
 - File name: **/opt/HiCommand/Base/HDB/.pdveritas**
 - Details: This is an empty file.
3. Create the script that defines the resource types for the HiRDB service.
 - File name: **/etc/VRTSvcs/conf/config/HiRDB_STypes.cf**
 - Details: Create a file containing the following:

```
type HiRDB_S (  
static str ArgList[] = { PdDir, PdConfPath, Ld_Library_Path, DummyFilePath }  
str PdDir  
str PdConfPath  
str Ld_Library_Path  
str DummyFilePath)
```

4. Define the agent for HiRDB.

```
# mkdir /opt/VRTSvcs/bin/HiRDB_S
# cp /opt/VRTSvcs/bin/ScriptAgent /opt/VRTSvcs/bin/HiRDB_S/HiRDB_SAgent
```

5. Create the script that is used to put the HiRDB service online.
 - File name: **/opt/VRTSvcs/bin/HiRDB_S/online**
 - Details: Create a file containing the following:

```
#!/bin/sh
PATH=/sbin:/usr/bin:/usr/sbin:/etc:/bin:/opt/VRTSvcs/bin:"$2"/bin
export PATH
PDDIR="$2"
PDCONFPATH="$3"
LD_LIBRARY_PATH="$4"
export PDDIR PDCONFPATH LD_LIBRARY_PATH
$PDDIR/bin/pdstart
/bin/touch "$5"
/bin/chmod 0400 "$5"
```

6. Create the script that is used to place the HiRDB service offline.
 - File name: **/opt/VRTSvcs/bin/HiRDB_S/offline**
 - Details: Create a file containing the following:

```
#!/bin/sh
PATH=/sbin:/usr/bin:/usr/sbin:/etc:/bin:/opt/VRTSvcs/bin:"$2"/bin
export PATH
PDDIR="$2"
PDCONFPATH="$3"
LD_LIBRARY_PATH="$4"
export PDDIR PDCONFPATH LD_LIBRARY_PATH
$PDDIR/bin/pdstop -f -q
/bin/rm -f "$5"
```

7. Create the script that is used to monitor the HiRDB service.
 - File name: **/opt/VRTSvcs/bin/HiRDB_S/monitor**
 - Details: Create a file containing the following:

```
#!/bin/sh
if /bin/test -f "$5"
then
    exit 110
else
    exit 100
fi
```

8. Assign execution permissions to the created scripts.
 - **# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/online**
 - **# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/offline**
 - **# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/monitor**

4.5.3.4 Creating Scripts for Sun Cluster

After installing and setting up HiCommand Device Manager on the executing node and standby node, you must create the script for registering Common Component service in the cluster on both nodes.

Create the following six script files:

1. Create the script for HBase Storage Management Web Service.

- File name: **/etc/init.d/sc_hicommand-CWS**
- Details: Create a file containing the following:

```
#!/bin/sh
#
# Sample sc_hicommand-CWS
#
# Usage: sc_hicommand-CWS [start|stop|status]
#
# This Script executes /etc/init.d/hicommand-CWS internally.
ALIVE_VALUE=0
DOWN_VALUE=1
exec_cmd() {
    echo `date "+%y/%m/%d %H:%M:%S" ` "exec : $*"
    # Execute Command with operand
    $*
    # Set return value to RC
    RC=$?
    echo `date "+%y/%m/%d %H:%M:%S" ` "exec-end: $* (RC=$RC)"
    if [ $RC -ne 0 ]; then
        if [ $RC -ne 1 ]; then
            exit $RC
        fi
    fi
}

# Switch operation according to the first operand of this shell.
case $1 in
start)
    exec_cmd "/etc/init.d/hicommand-CWS start"
    ;;
stop)
    exec_cmd "/etc/init.d/hicommand-CWS stop"
    ;;
status)
    /etc/init.d/hicommand-CWS status
    # The result is equal to 1
    if [ $? -eq 1 ]; then
        # running
        RET_CODE=$ALIVE_VALUE
    else
        # not running
        RET_CODE=$DOWN_VALUE
    fi
    exit $RET_CODE
    ;;
*)
    echo "Invalid argument"
    exit 1
esac

exit 0
```

2. Create a script for the HBase Storage Mgmt Common Service.

- File name: **/etc/init.d/sc_hicommand-SSOS**
- Details: Create a file containing the following:

```
#!/bin/sh
#
# Sample sc_hicommand-SSOS
#
# Usage: sc_hicommand-SSOS [start|stop|status]
#
# This Script executes /etc/init.d/hicommand-SSOS internally.
ALIVE_VALUE=0
DOWN_VALUE=1

exec_cmd() {
    echo `date "+%y/%m/%d %H:%M:%S "` `exec    : $*`
    # Execute Command with operand
    $*
    # Set return value to RC
    RC=$?
    echo `date "+%y/%m/%d %H:%M:%S "` `exec-end: $* (RC=$RC)`
    if [ $RC -ne 0 ]; then
        if [ $RC -ne 1 ]; then
            exit $RC
        fi
    fi
}

# Switch operation according to the first operand of this shell.
case $1 in
start)
    exec_cmd "/etc/init.d/hicommand-SSOS start"
    ;;
stop)
    exec_cmd "/etc/init.d/hicommand-SSOS stop"
    ;;
status)
    /etc/init.d/hicommand-SSOS status
    # The result is equal to 1
    if [ $? -eq 1 ]; then
        # running
        RET_CODE=$ALIVE_VALUE
    else
        # not running
        RET_CODE=$DOWN_VALUE
    fi
    exit $RET_CODE
    ;;
*)
    echo "Invalid argument"
    exit 1
esac

exit 0
```

3. Create a script for starting HiRDB.

- File name: **/etc/init.d/hirdb_start**
- Details: Create a file containing the following:

```
#!/bin/sh
PATH=/usr/sbin:/usr/bin:$PDDIR/bin:./usr/cluster/bin
export PATH
PDDIR=/opt/HiCommand/Base/HDB
PDCONFPATH=$PDDIR/conf
LD_LIBRARY_PATH=$PDDIR/lib
PDHOST=logical-host-name
export PDDIR PDCONFPATH LD_LIBRARY_PATH PDHOST

$PDDIR/bin/pdstart
```

```
/etc/init.d/hirdb_monitor
```

4. Create a script for stopping HiRDB.

- File name: **/etc/init.d/hirdb_stop**
- Details: Create a file containing the following:

```
#!/bin/sh

PATH=/usr/sbin:/usr/bin:$PDDIR/bin:./usr/cluster/bin
export PATH
PDDIR=/opt/HiCommand/Base/HDB
PDCONFPATH=$PDDIR/conf
LD_LIBRARY_PATH=$PDDIR/lib
PDHOST=logical-host-name
export PDDIR PDCONFPATH LD_LIBRARY_PATH PDHOST

$PDDIR/bin/pdstop -f -q
```

5. Create a script for monitoring HiRDB.

- File name: **/etc/init.d/hirdb_probe**
- Details: Create a file containing the following:

```
#!/bin/sh

ps -ef | grep root | grep pdprcd | awk -F' ' '{print $8}' | grep pdprcd
if [ $? = 0 ];then
    echo "exit 0"
    exit 0
else
    echo "exit 1"
    exit 1
fi
```

6. Create a HiRDB resident script.

- File name: **/etc/init.d/hirdb_monitor**
- Details: Create a file containing the following:

```
#!/bin/sh

trap exit 5
while true
do
    sleep 5
done
exit
```

7. After creating the scripts, assign execution permissions to the scripts using the following command:

chmod u+x script-file-name

4.5.3.5 Setting Up the Cluster Resource for VERITAS Cluster Server

If you are using Sun Cluster Server, skip this section and go to section 4.5.3.6.

To set the cluster resources, do the following operation on the executing node or the standby node:

1. In Java Console, start Cluster Manager.
2. Open the VERITAS Cluster Server configuration file so that you can edit the file. From the **File** menu, choose **Open Configuration**.
3. Import the file created in section 4.5.3.3. From the **File** menu, choose **Import Types**.
4. Select the **/etc/VRTSvcs/conf/config/HiRDB_STypes.cf** file, and then choose **Import**.
5. If there is no group to which other HiCommand Suite products are registered, create the service group. In the **Edit** menu, select **Add** and then **Service Group**.
Caution: Use only resources related to HiCommand Suite products to configure the resource group.
 - In Service Group Name, enter **HiCommand**.
 - Move both the executing and standby nodes from **Available Systems** to **Systems for Service Group**.
 - Select **OK**.
6. In the **Add New Resource** dialog box, from **Resource Type** choose **IP**, and then register the IP address (cluster management IP address) used to access the Device Manager Server.
7. Register a shared disk into the HiCommand group: In the **Add New Resource** dialog box, from **Resource Type** choose **Disk Reservation** to register device files on the shared disk. Enter **SharedDisk** for the resource name.
8. Register a mount point: In the **Add New Resource** dialog box, from **Resource Type** choose **Mount** to register the mount point on the shared disk. Enter **MountPoint** for the resource name.
9. In the **Edit** menu, select **Add** and then **Resource** to display the **Add Resource** panel.
10. Register HiRDB as a resource, as follows:
 - Resource Name: **HiRDB** (optional)
 - Resource Type: **HiRDB_S**
 - PdDir: **/opt/HiCommand/Base/HDB**
 - PdConfPath: **/opt/HiCommand/Base/HDB/conf**
 - Ld_Library_Path: **/opt/HiCommand/Base/HDB/lib**
 - DummyFilePath: **/opt/HiCommand/Base/HDB/.pdVERITAS**
 - Critical: **false**
11. Register the HBase Storage Mgmt Common Service as a resource, as follows:
 - Resource Name: **MgmtComService** (optional)
 - Resource Type: **Application**
 - Start Program Attribute: **Scalar Values:/etc/init.d/hicommand-SSOS start**
 - Stop Program Attribute: **Scalar Values:/etc/init.d/hicommand-SSOS stop**

- PidFiles Attribute: **/var/opt/HiCommand/Base/tmp/HiCommand.pid**
12. Register the HBase Storage Mgmt Web Service as a resource, as follows:
- Resource Name: **MgmtWebService** (optional)
 - Resource Type: **Application**
 - Start Program Attribute: **Scalar Values:/etc/init.d/hicommand-CWS start**
 - Stop Program Attribute: **Scalar Values:/etc/init.d/hicommand-CWS stop**
 - PidFiles Attribute: **/var/opt/HiCommand/Base/httpsd/logs/httpd.pid**

13. Register the Device Manager Server as a resource, as follows:

- Resource Name: **HiCommandServer** (optional)
- Resource Type: **Application**
- Start Program Attribute: **Scalar Values:/etc/init.d/hicommand start**
- Stop Program Attribute: **Scalar Values:/etc/init.d/hicommand stop**
- Monitor Processes Attribute:
Vector Values:/bin/sh /opt/HiCommand/HiCommandServer/hicmdserver

Caution: If HiCommand Suite Common Component is forcibly stopped for any reason, some temporary files will be left undeleted. If these files are on the standby node, even if HiCommand Suite Common Component has stopped, a message indicating that HiCommand Suite Common Component cannot be placed offline is output to the VERITAS Cluster Server log. Even though this error message is output, there is no problem with the Device Manager server operation.

To prevent the error message from being output, make sure the Common Component is not running by executing the following command:

/opt/HiCommand/Base/bin/hcmdssrv -status

Then do the following:

- Delete **HiCommand.pid** from the **/var/opt/HiCommand/Base/tmp** directory
- Delete **httpd.pid** from the **/var/opt/HiCommand/Base/httpsd/logs** directory

14. Set up the resource dependency in the HiCommand group in the following order. The lower resource depends on the upper resources:

- Device files on the shared disk
- Mount point on the shared disk and IP address
- HiRDB
- HiCommand Storage Mgmt Common Service
- HiCommand Storage Mgmt Web Service
- HiCommandServer

The above resource names are represented by the resource names registered from step 11 to step 13.

15. From the File menu, choose **Save Configuration**.

16. From the File menu, choose **Close Configuration**.

17. Apply the resource, and then close Cluster Manager.

4.5.3.6 Setting Up the Cluster Resource for Sun Cluster

To register resources for Sun Cluster, use the **scrgadm** command. For more information, see the Sun Cluster documentation.

Execute the following operation on the executing node or standby node:

1. If there is no group to which other HiCommand Suite products are registered, create a resource group:

- Group name: **HiCommand**
- Node: A host name of the executing node and host name of the standby node.
- Sample command: **# /usr/cluster/bin/scrgadm -a -g HiCommand -h <executing node host name>,<standby node host name>**

Caution: Use only resources related to HiCommand Suite products to configure the resource group.

2. Register the shared disk as a resource:

- Resource type: **SUNW.HAStoragePlus**
- Resource name: **SharedDisk**

3. Register a logical host name as a resource:

- Resource name: **hdvm_ip**

4. Register HiRDB as a resource:

- Resource type: **SUNW.gds**
- Resource name: **HiRDB** (optional)
- Related network: **hdvm_ip**
- Resources on which HiRDB depends: **SharedDisk**
- Start command for the service: **/etc/init.d/hirdb_start**
- Stop command for the service: **/etc/init.d/hirdb_stop#**
- Monitoring command for the service: **/etc/init.d/hirdb_probe#**
- Port number to be used: **23032/tcp**

Note: For the service startup, stop and monitoring commands, register the script created in section 4.5.3.4, as follows:

```
# /usr/cluster/bin/scrgadm -a -j HiRDB -g HiCommand -t SUNW.gds
-y Network_resources_used=hdvm_ip
-y Resource_dependencies=SharedDisk
-x Start_command="/etc/init.d/hirdb_start"
-x Stop_command="/etc/init.d/hirdb_stop"
-x Probe_command="/etc/init.d/hirdb_probe"
-y Port_list="23032/tcp"
```

5. Register HBase Storage Mgmt Common Service as a resource:

- Resource type: **SUNW.gds**
- Resource name: **MgmtComService** (optional)
- Related network: **None**
- Resources on which HBase Storage Mgmt Common Service depends: **HiRDB**
- Start command for the service: **/etc/init.d/sc_hicommand-SSOS start**
- Stop command for the service: **/etc/init.d/sc_hicommand-SSOS stop**
- Monitoring command for the service: **/etc/init.d/sc_hicommand-SSOS status**
- Port number to be used: **23017/tcp**

Note: /etc/init.d/sc_hicommand-SSOS must be created in advance. For more information see section 4.5.3.4.

Sample command:

```
# /usr/cluster/bin/scrgadm -a -j MgmtComService -g HiCommand
-t SUNW.gds -y Resource_dependencies=HiRDB
-x Start_command="/etc/init.d/sc_hicommand-SSOS start"
-x Stop_command="/etc/init.d/sc_hicommand-SSOS stop"
-x Probe_command="/etc/init.d/sc_hicommand-SSOS status"
-y Port_list="23017/tcp"
```

6. Register HBase Storage Mgmt Web Service as a resource:

- Resource type: **SUNW.gds**
- Resource name: **MgmtWebService** (optional)
- Related network: **hdvm_ip**
- Resources on which HBase Storage Mgmt Web Service depends: **MgmtComService**
- Start command for the service: **/etc/init.d/sc_hicommand-CWS start**
- Stop command for the service: **/etc/init.d/sc_hicommand-CWS stop**
- Monitoring command for the service: **/etc/init.d/sc_hicommand-CWS status**
- Port number to be used:
 - Other than SSL: 23015/tcp
 - For SSL: **23016/tcp**

Note: /etc/init.d/sc_hicommand-CWS must be created in advance. For more information, see section 4.5.3.4.

Sample command:

```
# /usr/cluster/bin/scrgadm -a -j MgmtWebService -g HiCommand -t SUNW.gds
-y Network_resources_used=hdvm_ip
-y Resource_dependencies=MgmtComService
-x Start_command="/etc/init.d/sc_hicommand-CWS start"
-x Stop_command="/etc/init.d/sc_hicommand-CWS stop"
-x Probe_command="/etc/init.d/sc_hicommand-CWS status"
-y Port_list="23015/tcp"
```

7. Register HiCommandServer as a resource:

- Resource type: **SUNW.gds**

- Resource name: **HiCommandServer** (optional)
- Related network: **hdvm_ip**
- Resources on which HiCommandServer depends: **MgmtWebService**
- Start command for the service: **/etc/init.d/hicommand start**
- Stop command for the service: **/etc/init.d/hicommand stop**
- Monitoring command for the service: **/etc/init.d/hicommand status2**
- Port number to be used:
 - Not for SSL: **2001/tcp**
 - For SSL: **2443/tcp**

Sample command:

```
# /usr/cluster/bin/scrgadm -a -j HiCommandServer -g HiCommand -t SUNW.gds
-y Network_resources_used=hdvm_ip
-y Resource_dependencies=MgmtWebService
-x Start_command="/etc/init.d/hicommand start"
-x Stop_command="/etc/init.d/hicommand stop"
-x Probe_command="/etc/init.d/hicommand status2"
-y Port_list=2001/tcp
```

4.5.4 Performing an Upgrade Installation from Version 3.5 or Earlier

This section describes how to upgrade the Device Manager version 3.5 or earlier in a VERITAS Cluster Server configuration to Device Manager 4.0 or later.

Caution: Upgrade VERITAS Cluster Server to version 4.0 before upgrading HiCommand Device Manager.

After finishing an upgrade installation, be sure to back up the HiCommand Device Manager server database.

4.5.4.1 Preparations in VERITAS Cluster Server

To prepare VERITAS Cluster Server in advance, execute the following operation on the executing node or standby node:

1. In Java Console, start the VERITAS Cluster Manager.
2. In the Cluster Explorer panel, select the **Service Groups** tab.
3. Take each of the following services offline, by selecting each of the following services, right-clicking to display a menu, selecting **Offline**, and then selecting **Host Name**:
 - HiCommand Server
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service

The above services are represented by the resource names registered in section 4.5.3.5.

4. Select each of the preceding services, right-click to display a menu, and then deselect **Enabled**.
5. Select the group to which the Device Manager Server service has been registered, right-click to display a menu, and select **Freeze** and then **Temporary**.

4.5.4.2 Upgrading Device Manager on the Executing Node

This section describes how to upgrade Device Manager from version 3.5 or earlier to version 4.0 or later.

WARNING: If you have made any changes to `/opt/HiCommand/Base/conf/init.conf`, and you are upgrading from Device Manager version 3.0 or 3.1 to version 3.5 or later, you must first create a new folder for **<common component installation folder>\conf\user.conf**, and duplicate those changes in this file.

1. Copy HBASE.GDB on the shared disk to the following directory on the standby node.
/var/opt/HiCommand/Base/database/
2. Copy HiCommand.gdb on the shared disk to the following directory on the standby node.
/opt/HiCommand/HiCommandServer/database/interbase
3. On the executing node, perform an upgrade installation of the Device Manager Server to version 4.0 or higher (see section 4.4.2). The following are the requirements for the installation:
 - Leave the settings specifying the location of the databases for the Common Component and Device Manager Server as the default values (see Figure 4.9 and Figure 4.10).
 - Perform database conversion during the installation. (see Figure 4.25)
4. Use a text editor to create a cluster configuration file.
 - `virtualhost`: Specify the logical host name.
 - `onlinehost`: Specify the host name of the executing node.
 - `standbyhost`: Specify the host name of the standby node
 - `mode = online`.

Sample command:

```
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
mode = online
```

5. Save the created file as `cluster.conf` in **/opt/HiCommand/Base/conf**.
Caution: You cannot specify an IP address for **virtualhost**, **onlinehost**, or **standbyhost**. Confirm that the IP address can be resolved from the host name.
6. Stop the Device Manager Server and Common Component using the following command.
/opt/HiCommand/suitesrvctl -stop_all

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

7. Start HiRDB using the following command.

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

8. Back up the database. See section 4.8.1 if you need instructions.
9. Migrate the database to the shared disk.

Delete or empty *target-directory-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -createcluster -databasepath
target-directory-for-recreating-database -exportpath target-directory-for-storing-
data
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -createcluster -databasepath
/root/re_creating_db -exportpath /opt/storing_data
```

Caution: Specify an absolute path (63 bytes maximum) for *target-directory-for-recreating-database* and *target-directory-for-storing-data*.

Caution: *target-directory-for-recreating-database* must be placed on a shared disk. *target-directory-for-storing-data* must be placed on your local disk.

Caution: The characters that can be used for *target-directory-for-recreating-database* and *target-directory-for-storing-data* are as follows. In addition to these characters, a forward slash (/) can be used as a path delimiter. You cannot use a space in a path.

A-Z a-z 0-9 . _

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

10. If HiCommand Suite Common Component is running, execute the following command to stop it.

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

11. Set the Common Component so that it does not start automatically when the machine starts.

```
# /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all
```

12. Set the Device Manager Server so that it does not start automatically when the machine starts, by moving the following file to another directory, or changing its file name.

```
/etc/rc3.d/S99hicommand
```

Note: When changing the file name, do not use a name beginning with K or S.

4.5.4.3 Upgrading HiCommand Device Manager on Standby Node

1. Start InterBase Server.

/etc/init.d/interbaseserver start

2. Use a text editor to open the following file.

/opt/HiCommand/HiCommandServer/config/database.properties

3. Change the line beginning with dbm.url= as shown below:

dbm.url=jdbc:interbase://localhost//opt/HiCommand/HiCommandServer/database/interbase/HiCommand.gdb

4. Use a text editor to open the following file. (If the file does not exist, create the file.)

/opt/HiCommand/Base/conf/user.conf

5. Change the line beginning with DATABASE.path= as shown below:

DATABASE.path=/var/opt/HiCommand/Base/database/HBASE.GDB

Note: If no line begins with DATABASE.path=, add the line.

6. On the standby node, perform an upgrade installation of HiCommand Device Manager Server (see section 4.4.2 if you need instructions). The following are the requirements for the installation:
 - Leave the settings specifying the location of the databases for the Common Component and the Device Manager Server as the default values. (see Tables 4-9 and 4-10)
 - If you are upgrading from version 4.0 or higher, do not convert the database (see Figure 4.25).
7. Create the cluster configuration file. Specify the following items in the cluster configuration file:
 - mode: Specify online for the executing node, and standby for the standby node.
 - virtualhost: Specify the logical host name.
 - onlinehost: Specify the host name of the executing node.
 - standbyhost: Specify the host name of the standby node.

Sample command:

```
mode = standby
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

8. Save the created file as cluster.conf in **/opt/HiCommand/Base/conf**.

Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

9. Stop the Device Manager Server and Common Component using the following command.

/opt/HiCommand/suitesrvctl -stop_all

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

10. Change the setting so that the database system on the shared disk is to be referenced.

When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

/opt/HiCommand/Base/bin/hcmdsdbrmake -cluster -databasepath target-directory-for-recreating-database

The following shows an example of executing the command:

/opt/HiCommand/Base/bin/hcmdsdbrmake -cluster -databasepath /root/re_creating_db

Caution: Specify the same target directory for re-creating the database as on the executing node. Do not specify a path that includes a space.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

11. If HiCommand Suite Common Component is running, execute the following command to stop it.

/opt/HiCommand/Base/bin/hcmdssrv -stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

12. Set the Common Component so that it does not start automatically when the machine starts.

/opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

13. Set the Device Manager Server so that it does not start automatically when the machine starts.

/etc/rc3.d/S99hicommand

Note: When changing the file name, do not use a name beginning with K or S.

4.5.4.4 Creating Scripts for HiRDB

After upgrading Device Manager on the executing node and standby node, you must create the script for HiRDB on both nodes. The procedure is the same as for an initial installation. For more information, see section 4.5.3.3.

4.5.4.5 Setting Up the Cluster Resource

1. In Java Console, start Cluster Manager.
2. In the Cluster Explorer window, select the **Service Groups** tab. Right-click the group to which the Device Manager services have been registered, and then choose **Unfreeze**.
3. In the Cluster Explorer panel, select the **Service Groups** tab. Select **InterBase services**, right-click to display a menu, and then select **Delete**.

Note: Do not delete these resources if other resources depend on them.

4. For each of the following service parameters, specify the same value as for a new installation. For more information, see section 4.5.3.5.

- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- Device Manager Server

The above services are represented by the resource names registered in section 4.5.3.5.

5. On both the executing and standby nodes, delete the following files:

- **/etc/init.d/cluster_hicommand-SSOS**
- **/etc/init.d/cluster_hicommand-CWS**

6. Register the HiRDB service to the group to which the HiCommand Device Manager service has been registered. Use the same procedure as for a new installation. For more information, see section 4.5.3.5.
7. On the executing node, place online the group to which the HiCommand Device Manager service is registered.

4.5.5 Performing an Upgrade Installation from Version 4.0 or Later or Performing a Re-installation

This section describes how to perform an upgrade installation of HiCommand Device Manager from version 4.0 or later and how to re-install the same version of HiCommand Device Manager by overwriting in a VERITAS Cluster Server or Sun Cluster cluster environment.

Warning: After finishing an upgrade installation or re-installation, make sure to back up the HiCommand Device Manager server database.

WARNING: Before performing an upgrade installation or re-installation, you must confirm that the services on the executing node are online.

4.5.5.1 Preparing for Re-installation in VERITAS Cluster Server

Note: If you are using Sun Cluster, skip this section and go to section 4.5.5.2.

To prepare for re-installation, perform the following operations on the executing node:

1. In Java Console, start Cluster Manager.
2. Place the following services offline:
 - Device Manager Server
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service

The above services are represented by the resource names registered in section 4.5.3.5.

3. For each of the preceding services, right-click to display a menu, and then deselect **Enabled**.
4. Stop the Common Component using the following command:

/opt/HiCommand/Base/bin/hcmdssrv -stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

5. Place the HiRDB service offline by selecting the HiRDB service, right-clicking to display a menu, and then deselecting **Enabled**.
6. In the Cluster Explorer window, select the **Service Groups** tab.
7. Right-click the group to which the Device Manager services have been registered. Choose **Freeze** and then **Temporary**.

4.5.5.2 Preparing for Re-installation in Sun Cluster

Execute the following operations on the executing node:

1. Disable monitoring of the resources of the HBase Storage Mgmt Web Service, HiCommand Server, and HBase Storage Mgmt Common Service.

```
# /usr/cluster/bin/scswitch -n -M -j MgmtWebService
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j SMgmtComService
```

For the resource names in the above commands, specify the resource names registered in section 4.5.3.6.

2. Execute the following command to disable the HBase Storage Mgmt Web Service, HiCommand Server, and HBase Storage Mgmt Common Service.

```
# /usr/cluster/bin/scswitch -n -j MgmtWebService
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j MgmtComService
```

For the resource names in the above commands, specify the resource names registered in section 4.5.3.6.

3. Stop the Common Component on the executing node.

/opt/HiCommand/Base/bin/hcmdssrv -stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

4. Disable monitoring of the HiRDB resource.

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

For the resource names in the above commands, specify the resource names registered in section 4.5.3.6.

5. Disable the HiRDB resource.

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

For the resource names in the above commands, specify the resource names registered in section 4.5.3.6.

4.5.5.3 Performing an Upgrade or Re-installation of Device Manager on the Executing Node

1. Perform an upgrade installation or re-installation of the HiCommand Device Manager server (see section 4.5.5).

Caution: During the upgrade installation or re-installation, backup or export the database.

2. Stop the Device Manager Server and Common Component.

/opt/HiCommand/suitesrvctl -stop_all

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

3. Set the Common Component service so that it does not start automatically when the machine starts.

/opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

4. Set the Device Manager Server so that it does not start automatically when the machine starts.

/etc/rc3.d/S99hicommand

Note: Make sure that the file name does not start with K or S.

5. Place the group to which the HiCommand Device Manager service has been registered on standby.
6. If you are using the VERITAS Cluster Server, do the following:
 - In the Cluster Explorer panel, select **Service Groups**.
 - Select the group to which the HiCommand Device Manager service has been registered.
 - Right-click to display a menu.
 - Select **Unfreeze**.
 - Choose **Switch To**, and then **Host Name**.
 - Choose **Freeze**, and then **Temporary**.
7. If you are using the Sun Cluster Server, execute the following command:

/usr/cluster/bin/scswitch -z -g group-name -h host-name

4.5.5.4 Perform an Update or Re-installation of Device Manager on the Standby Node

1. Perform an update installation or re-installation of the HiCommand Device Manager server (see section 4.5.5).

Caution: When a message appears prompting you to confirm whether you want to back up a database or whether you want to export a database, do not select **y**. If you select **y**, installation fails.

2. Stop the Device Manager Server and the Common Component.

/opt/HiCommand/suitesrvctl -stop_all

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

3. Set the Common Component service so that it does not start automatically when the machine starts.

/opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

4. Set the Device Manager Server so that it does not start automatically when the machine starts by moving the following file to another directory, or changing its file name:

/etc/rc3.d/S99hicommand

Note: Make sure that the file name does not start with K or S.

4.5.5.5 Configuring the VERITAS Cluster Server

1. In Java Console, start Cluster Manager.
2. Access the Cluster Explorer panel.
3. Select the **Service Groups** tab.
4. Select the group to which HiCommand Device Manager service has been registered.
5. Right-click to display a menu, then select **Unfreeze**.
6. Select the group to which the HiCommand Device Manager service has been registered, right-click to display a menu, and select **Enable Resources**.
7. From the **File** menu, choose **Save Configuration**, and then **Close Configuration**.
8. On the executing node, place online the group where the Device Manager service is registered.

4.5.5.6 Configuring the Sun Cluster

1. Apply the Common Component and HiCommand Device Manager services.

```
/usr/cluster/bin/scswitch -e -j HiRDB  
/usr/cluster/bin/scswitch -e -j MgmtComService  
/usr/cluster/bin/scswitch -e -j MgmtWebService  
/usr/cluster/bin/scswitch -e -j HiCommandServer
```

For the resource names in the above commands, specify the resource names registered in section 4.5.3.6.

2. Apply the monitoring of the Common Component and HiCommand Device Manager services.

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB  
# /usr/cluster/bin/scswitch -e -M -j MgmtComService  
# /usr/cluster/bin/scswitch -e -M -j MgmtWebService  
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
```

For the resource names in the above commands, specify the resource names registered in section 4.5.3.6.

3. In Java Console, start Cluster Manager.
4. On the executing node, place online the group where the Device Manager service is registered.

4.5.6 Converting to a Cluster Configuration

Caution: HiCommand Device Manager server only supports Solaris cluster environments.

This section contains instructions for changing to a cluster configuration after you have already started operating under a non-cluster configuration. In this example, the Device Manager Server where operations are already running is treated as the executing node.

1. On the host that will be used as the standby node, install the Device Manager Server. see section 4.5 if you need instructions.

2. On the standby node, display the Web Client logon, then enter the license key.

Note: You should have received a CD that contains the HiCommand Device Manager License Key. Upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found simply highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.

3. On both the executing and standby nodes, stop the Device Manager server and the HiCommand Suite Common Component.

/opt/HiCommand/suitesrvctl -stop_all

4. In the executing node, start HiRDB by executing the following command.

/opt/HiCommand/Base/bin/hcmdsdbsrv -start

5. On both the executing and standby nodes, use a text editor to create a cluster configuration file for each node. Specify the following:
 - mode: Specify online for the executing node, and standby for the standby node.
 - virtualhost: Specify the logical host name.
 - onlinehost: Specify the host name of the executing node.
 - standbyhost: Specify the host name of the standby node.
 - mode = online.

Sample command:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

6. Save the created file as cluster.conf in **/opt/HiCommand/Base/conf**.

Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

7. Back up the database. See section 4.8.1 if you need instructions.

8. In the executing node, migrate the database to the shared disk.

Delete or empty *target-directory-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath
target-directory-for-recreating-database -exportpath target-directory-for-storing-
data
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath
/root/re_creating_db -exportpath /opt/storing_data
```

Caution: Specify an absolute path (63 bytes maximum) for *target-directory-for-recreating-database* and *target-directory-for-storing-data*.

Caution: *target-directory-for-recreating-database* must be placed on a shared disk. *target-directory-for-storing-data* must be placed on your local disk.

Caution: The characters that can be used for *target-directory-for-recreating-database* and *target-directory-for-storing-data* are as follows. In addition to these characters, a forward slash (/) can be used as a path delimiter. You cannot use a space in a path.

A-Z a-z 0-9 . _

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

9. On the standby node, change the settings so that a database on the shared disk is used.

Execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
# /opt/HiCommand/Base/bin/hcmdsdbremake -cluster -databasepath target-
directory-for-recreating-database
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbremake -cluster -databasepath
/root/re_creating_db
```

Caution: Specify the same directory as the directory specified for *target-directory-for-recreating-database* on the executing node. Do not specify a path that includes a space.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

10. If HiCommand Suite Common Component is running on both the executing node and standby nodes, execute the following command to stop it.

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

11. Set the Common Component service so that it does not start automatically when the machine starts.

```
# /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all
```

12. Set the Device Manager Server so that it does not start automatically when the machine starts.

/etc/rc3.d/S99hicommand

Note: Make sure that the file name does not start with K or S.

13. Complete setting up the cluster environment. For more information, see section 4.5.

4.6 Verifying HiCommand Device Manager Installation

This section describes the procedure for verifying that the Device Manager server and HiCommand Suite Common Component have been installed correctly.

Caution: Even if installation of HiCommand Device Manager fails, the **GO** menu command for starting HiCommand Device Manager might appear in the Dashboard of other HiCommand Suite products. To remove **GO**, a user with User Management permissions must execute the following command. When this command is executed, the HiCommand Suite Common Component services must be running.

```
# /opt/HiCommand/Base/bin/hcmdsintg -delete -type DeviceManager -user user-ID -pass password
```

4.6.1 Verifying the HiCommand Device Manager Server Installation

1. Enter the following command to verify that Device Manager is running.

/opt/HiCommand/suitesrvctl -status_hdvm

2. This command outputs several lines of text.

The first line of text should read HiCommand process ID: xxxx (xxxx is a number representing the process ID for the Device Manager daemon). If this is what you see, the installation was successful and Device Manager is up and running normally.

If you see HiCommand is not running, this indicates a problem. For more information about problem solving for Device Manager installation, see Chapter 10. If the problem has been resolved, execute the following command to start HiCommand Device Manager manually.

/opt/HiCommand/suitesrvctl -start_hdvm

4.6.2 Verifying HiCommand Suite Common Component Installation

1. Execute the following command to check whether HiCommand Suite Common Component is running:

/opt/HiCommand/Base/bin/hcmdssrv -status

2. If the following messages appear, the Common Component is running normally.

```
KAPM06440-I The HiRDB service has already started.
KAPM05007-I Already started service. service-name=HBase Storage
Mgmt Web Service
KAPM05007-I Already started service. service-name=HBase Storage
Mgmt Common Service
```

3. If the Common Component is not running, execute the following command to start it.
/opt/HiCommand/Base/bin/hcmdssrv -start
4. If the Common Component fails to start, the port number might already be in use. If this is the case, change the port number. See section 5.4.2 for instructions on how to change the port.

Another possible cause for the Common Component failing to start is the insufficient installed memory. To increase the amount of installed memory, see section 4.1.1.

Alternately, process IDs for service processes of the Common Component might overlap. If they do, perform the following operations:

 - Stop the Common Component (see section 5.2.2 if you need instructions).

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

 - Restart the Common Component.
<common component installation folder>\bin\hcmdssrv /start
 - If the Common Component still does not start, stop the Common Component again.
/opt/HiCommand/Base/bin/hcmdssrv -stop
 - Delete the following files.
/usr/bin/rm -rf /var/opt/HiCommand/Base/tmp/*.pid
 - Start the Common Component.
<common component installation folder>\bin\hcmdssrv /start
5. If the Common Component still does not start, restart the Device Manager server.

If the Common Component still fails to start, use the **hcmdsgetlogs** command to collect maintenance information, and then contact Customer Support. For more information on the **hcmdsgetlogs** command, see section 10.2.1.
6. If one or both of these processes are still not running, please check the install log and follow the instructions.
7. If the problem remains, uninstall Device Manager (see section 4.8.4 for instructions), reboot the system, and re-install Device Manager.

4.7 Starting and Stopping Device Manager Server

WARNING: If a Device Manager client (for example, Web Client, Device Manager CLI, or Device Manager Agent) is accessing the Device Manager Server when that machine is shut down, the Device Manager client processing will terminate. Make sure that Device Manager clients are not accessing the server before shutting down a machine that is running the Device Manager Server.

Note: Device Manager server 5.0 or later can not only start and stop independently, but it can also start or stop HiCommand Suite Common Component synchronously. In addition, a synchronized Device Manager server and HiCommand Suite Common Component can be restarted automatically after they are stopped.

The following shows how to perform start, stop, or other operations for the HiCommand Device Manager server and HiCommand Suite Common Component:

- To start the Device Manager Server, execute the following command:

/opt/HiCommand/suitesrvctl-start_hdvm

This command outputs several lines of text. The first line of text should read:

HiCommand process ID: xxxx. This indicates that Device Manager is up and running normally.

Note: xxxx is a number representing the process ID for the Device Manager daemon.

- To stop the Device Manager Server, enter the command:

/opt/HiCommand/suitesrvctl -stop_hdvm

- To check the status of the Device Manager Server, enter one of the following commands:

/opt/HiCommand/suitesrvctl -status_hdvm

/opt/HiCommand/hicommand.sh status2

Note: status2 is an interface used by other applications to check the status of the Device Manager Server. The result will be a return code, as described in Table 4.8.

Table 4.8 status2 Return Codes

Return Code	Description
0	Startup operations for the Device Manager Server have finished.
1	The HiCommand Device Manager server is not running.
2	The HiCommand Device Manager server is running.
3-99	Other status.
100	The server.properties file was not found.
101-199	External error.
200	The value of server.http.port in the server.properties file is invalid.
201-999	External error.
1000-65535	Internal error.

- To start the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

/opt/HiCommand/suitesrvctl -start_all

- To stop the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

/opt/HiCommand/suitesrvctl -stop_all

- To restart the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

```
# /opt/HiCommand/suitesrvctl -restart_all
```

- To check the status of the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

```
# /opt/HiCommand/suitesrvctl -status_all
```

Caution: Do not execute the `hicommand`, `hcmdssrv`, or `suitesrvctl` command while the `suitesrvctl` command is being executed. If you do so, the `suitesrvctl` command may not operate correctly. If you have done so inadvertently, re-execute the `suitesrvctl` command. Also, do not execute the `suitesrvctl` command while the `hicommand` or `hcmdssrv` command is being executed.

4.8 Operating the HiCommand Device Manager Server Database

This section describes how to perform the following operations for the Device Manager server database:

- Backing up
- Restoring the backed-up data
- Migrating the database (export and import)
- Initializing the database

The following table shows the differences in the functions between backing up and restoring verses exporting and importing.

Table 4.9 Backing Up and Restoring Verses Exporting and Importing

Item	Backing up and restoring	Exporting and importing
Conditions of the HiCommand Suite Common Component version	No limitation.	HiCommand Suite Common Component version 5.5 or later must be installed on the machine used for the export source or the import destination.
Main purpose of use	To recover the current operating environment when a failure occurs in the server machine.	To migrate the server machine from the current environment to a different environment (such as a machine with a different OS).
Target data	■ Databases for HiCommand Suite products ■ The HiCommand Suite Common Component database	■ Databases for HiCommand Suite products ■ User information included in the HiCommand Suite Common Component database
Conditions for the machine used for the restore destination or the import	The following must be the same in the backup source machine and the restore destination machine: ■ Types, versions, and revisions of the installed HiCommand Suite products	■ The HiCommand Suite products whose databases to be imported must be installed. ■ The versions of the installed HiCommand Suite products must be the same as or

destination	- Installation locations for each HiCommand Suite product, HiCommand Suite Common Component, each HiCommand Suite product database, and HiCommand Suite Common Component database - The IP address and host name of the machine	higher than the ones on the export source machine.
-------------	--	--

The following sections describe the procedure for each operation separately.

4.8.1 Backing Up the Server and Common Component Database

Caution: To back up the Device Manager database, a directory for storing the backup file is required. The capacity of this directory must be at least the total size of the following two directories:

- The directory storing the Device Manager database
- The directory storing the HiCommand Suite Common Component database

This capacity is a guideline value applied when only the Device Manager database is installed. If HiCommand Suite products other than Device Manager are also installed, take the capacities of those databases into account as well.

To back up a database:

1. From a terminal window, enter the following command to stop the Device Manager Server.

```
# /opt/HiCommand/suitesrvctl -stop_hdvm
```

2. Use the following command to verify that the Device Manager is not running:

```
# /opt/HiCommand/suitesrvctl -status_hdvm
```

3. The output of this command should display several lines of text. The second line of the output should display the text **HiCommand is not running**. If instead it displays a process ID, Device Manager is still running. Return to step 1 to stop the server.

4. Use the following command to confirm that HiRDB is running:

```
# /opt/HiCommand/Base/bin/hcmdssrv -status
```

This command outputs several lines of messages. If the following message is included, then HiRDB is running normally:

```
KAPM06440-I The HiRDB service has already started.
```

5. If HiRDB is not running, execute the following command:

```
# /opt/HiCommand/Base/bin/hcmdssrv -start
```

6. Execute the **hcmdsbackups** command from the terminal window.

```
# /opt/HiCommand/Base/bin/hcmdsbackups
```

The command format is as follows:

```
hcmdsbackups -dir <backup file target-directory>
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsbackups -dir /opt/db_bkup01
```

The specifiable options for this command are as follows:

dir

Specify the absolute path of the directory that stores backup files of the Device Manager Server database. Do not specify a path that includes a space.

Caution: Specify an empty directory for the dir option. If you specify a directory that is not empty, the backup processing will be aborted. In such a case, specify an empty directory, and then re-execute the **hcmdsbackups** command.

Note: When you execute the **hcmdsbackups** command, a directory named database will be created in the target directory for storing backup files, and the database backup file will be stored with the name **backup.hdb**.

7. Restart the Device Manager Server.

```
# /opt/HiCommand/suitesrvctl -start_hdvm
```

8. Verify that the Device Manager Server is running.

```
# /opt/HiCommand/suitesrvctl -status_hdvm
```

This command outputs several lines of text. The second line of text should read:

HiCommand process ID: xxxx. This indicates that HiCommand Device Manager is up and running normally.

4.8.2 Restoring the Server Database

Warning: Before restoring the database, be sure to confirm that the following are the same in the backup source Device Manager server and the restore destination Device Manager server. If the following are not the same, the database cannot be restored.

- Types, versions, and revisions of the installed HiCommand Suite products
- Installation location for each HiCommand Suite product, HiCommand Suite Common Component, each HiCommand Suite product database, and HiCommand Suite Common Component database
- The IP address and host name of the machines

To restore the database:

1. Stop the Device Manager Server.

```
# /opt/HiCommand/suitesrvctl -stop_hdvm
```

2. Verify that HiCommand Device Manager is not running.

```
# /opt/HiCommand/suitesrvctl -status_hdvm
```

3. The output of this command should display several lines of text. The second line of the output should display the text **HiCommand is not running**. If instead it displays a process ID, HiCommand Device Manager is still running. Return to step 1 to stop the Device Manager Server.

4. Stop HiRDB.

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

5. Verify that HiRDB is not running.

```
# /opt/HiCommand/Base/bin/hcmdssrv -status
```

6. This command outputs several lines of messages. If the following message is included, then HiRDB is not running:

KAPM06441-I The HiRDB service has already stopped.

7. Execute the **hcmdsdb** command from the terminal window.

- The execution destination is as follows:

```
# /opt/HiCommand/Base/bin/hcmdsdb
```

- The command format is as follows:

```
hcmdsdb -restore backup-file -type HiCommand-Suite-product-to-be-restored
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdb -restore /opt/db_bkup01/backup.hdb -type DeviceManager
```

- The specifiable options are as follows:

restore

- Specify the absolute path of the Device Manager Server database backup file (backup.hdb) acquired by the hcmdsbackups command. Do not specify a path that includes a space.

type

- Specify the name of the HiCommand Suite product to be restored. To restore the HiCommand(R) Device Manager database only, specify **DeviceManager**. To restore all the HiCommand Suite products databases at once, specify **ALL**. To restore the databases when you are uninstalling and then reinstalling all the HiCommand Suite products, specify **ALL**.

WARNING: If you do not want to restore the databases for other HiCommand Suite products, make sure that you specify **DeviceManager**.

8. If **DeviceManager** is specified for the type option, specify **true** for the value of the **server.base.initialsynchro** property in the **server.properties** file. For more information, see section 8.2.23.

9. Restart the Device Manager Server and Common Component with the following command:

```
# /opt/HiCommand/suitesrvctl -start_all
```

10. Verify that the Device Manager Server is running.

```
# /opt/HiCommand/suitesrvctl -status_hdvm
```

This command outputs several lines of text. The first line of text should read:

HiCommand process ID: xxxx. This indicates that the Device Manager Server is up and running normally.

4.8.3 Migrating the Server Database

If HiCommand Suite products are used for an extended period of time, you may need a higher performance machine in order to accommodate product version upgrades and the increased number of objects to be managed. If this occurs, database migration will be one important component of the machine replacement process. In HiCommand Suite products, you can migrate the database by using the `hcmdsdbtrans` command. The `hcmdsdbtrans` command migrates all information stored in the database of each HiCommand Suite product as well as user information managed by the HiCommand Suite Common Component.

You can use the `hcmdsdbtrans` command to migrate the Device Manager database to a machine that has a different environment than the currently operating server machine, as shown in the following cases:

- Migration to a different platform machine
- Migration to a machine on which the installation locations for HiCommand Suite products are different from the ones on the migration source
- Migration to a machine on which the versions of HiCommand Suite products are newer than the ones on the migration source

4.8.3.1 Notes When Migrating the Database

The following are notes for the types, versions, and user information of the HiCommand Suite products on the migration source and migration destination servers.

Notes for types and versions of the HiCommand Suite products on the migration source and migration destination servers:

- The database of a HiCommand Suite product that is not installed on the migration destination server cannot be migrated. Install all necessary HiCommand Suite products on the migration destination server.
- If any of the versions of the HiCommand Suite products installed on the migration destination server is older than the ones on the migration source server, the database cannot be migrated. On the migration destination server, install the HiCommand Suite products whose versions are the same as or higher than the ones on the migration source server.
- The database of Replication Monitor version 4.2 cannot be migrated. If you need to migrate this database, we recommend you upgrade the Replication Monitor to version 5.0 or later on both the migration source and destination servers beforehand.

Notes for user information:

- If there is user information on the migration destination server, this user information will be replaced with the user information from the migration source server. Therefore, do not perform a migration to the machine on which user information for the HiCommand suite products already exists.

- If the databases of several HiCommand Suite products installed on a management server are migrated in multiple operations, the user information is replaced with new information at each operation, and eventually only the user information for the products migrated during the last operation will remain. When you perform migration for multiple products, be sure to migrate the databases in one operation so that user information for every products can be migrated.
- You cannot perform migration to integrate the HiCommand Suite products that were running on multiple management servers on to one management server because user information will be overwritten with each successive migration.

4.8.3.2 Procedure for Migrating Databases

To migrate databases:

1. Install, on the migration destination server, the HiCommand Suite products whose databases will be migrated.
2. Export the databases at the migration source server by using the `hcmdsdbtrans` command.
3. Transfer the archive file from the migration source server to the migration destination server.
4. Import the database at the migration destination server by using the `hcmdsdbtrans` command.

The following sections describe the details of each procedure. To perform migration between heterogeneous platforms, also see section 3.7.3.

4.8.3.3 Installing the HiCommand Suite Products on the Migration Destination Server

Install, on the migration destination server, the HiCommand Suite products whose databases will be migrated. The version of each HiCommand Suite product installed on the migration destination server must be the same as or higher than the one on the migration source server.

4.8.3.4 Exporting the Database at the Migration Source Server

To export the database of Device Manager, a directory for temporarily storing the information of the database, and a directory for storing the archive file are required. Each of these directories requires the as much capacity as the total size of the following two directories:

- The directory storing the Device Manager database
- The directory storing the HiCommand Suite Common Component database (excluding the `sys` directory and the directories beneath it)

This capacity is a guideline value applied when only the Device Manager database is installed. If HiCommand Suite products other than Device Manager are also installed, take the capacities of those databases into account as well.

Caution: If the total capacity of the database exceeds 2 GB, an attempt to create the archive file fails when the database is exported. In this case, instead of using the archive file, transfer the database information collected when exporting the database, to the migration destination.

To export the database at the migration source server:

1. From a terminal window, execute the following command to stop the Device Manager server and HiCommand Suite Common Component:

```
# /opt/HiCommand/suitesrvctl -stop_all
```

Important: If other HiCommand Suite products are running, stop them all.

2. From the terminal window, execute the following command to start HiRDB:

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

3. From the terminal window, execute the `hcmdsdbtrans` command.

The default installation location of the `hcmdsdbtrans` command is as follows:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans
```

The command format is as follows:

```
hcmdsdbtrans -export -workpath working-directory -file archive-file
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans -export -workpath /opt/trans_work -file /opt/trans_file/db_arc
```

In the `hcmdsdbtrans` command, you can specify the following options:

`workpath`

Specify the absolute path to the working directory where you wish to temporarily store database information. Do not specify a path that includes a space. Specify a directory on your local disk.

Caution: Specify an empty directory for the `workpath` option. If you specify a directory other than an empty directory, export processing will be cancelled. If this occurs, specify an empty directory and execute the `hcmdsdbtrans` command again.

`file`

Specify the absolute path to the archive file of the database to be exported. Make sure that the absolute path does not include a space.

The following table lists the actions to be taken when an error message is output. If a message that does not have one of the following message IDs is output, take actions according to the message.

Table 4.10 Action to Be Taken When an Error Message Is Output (During an Export)

Message ID	Action
------------	--------

KAPM05909-E	Collect maintenance information, and then contact Customer Support.
KAPM05910-E	Make sure that the products have been properly installed, and if necessary, take actions to satisfy this condition. If an error still occurs after taking the above actions, collect maintenance information, and then contact Customer Support.
KAPM05922-E	Make sure that you secure sufficient space in the disk that is to store the archive file. If an error still occurs even after securing the disk space, collect maintenance information, and then contact Customer Support.
KAPM05923-E	Instead of the archive file, transfer the data stored in the directory specified by the <code>workpath</code> option to the migration destination server.

4. Transfer the exported file to the migration destination server.

If the archive file cannot be created, transfer all the files stored in the directory specified by the `workpath` option. In that case, do not change the file structure in the directory specified by the `workpath` option.

4.8.3.5 Importing the Database at the Migration Destination Server

Caution: If the OS of the migration destination server is Windows, follow the procedure in section 3.7.3.5.

To import the database at the migration destination server:

1. From a terminal window, execute the following command to stop the Device Manager server and HiCommand Suite Common Component:

```
# /opt/HiCommand/Base/bin/suitesrvctl -stop_all
```

Important: If other HiCommand Suite products are running, stop them all.

2. From the terminal window, execute the following command to start HiRDB.

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

3. From the terminal window, execute the `hcmdsdbtrans` command.

The default installation location of the `hcmdsdbtrans` command is as follows:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans
```

The format of the command is as follows:

```
hcmdsdbtrans -import -workpath working-directory [-file archive-file] -type {ALL |  
HiCommand-Suite-products-whose-databases-will-be-migrated}
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans -import -workpath /opt/trans_work -type  
ALL
```

In the `hcmdsdbtrans` command, you can specify the following options:

`workpath`

When using an archive file during the import:

Specify the absolute path to the directory used to extract the archive file. Do not specify a path that includes a space. Specify a directory on your local disk. If you use an archive file, the `file` option must be specified.

Caution: Specify an empty directory for the `workpath` option. If you specify a directory other than an empty directory, export processing will be cancelled. If this occurs, specify an empty directory, and then execute the `hcmdsdbtrans` command again.

When not using the archive file during the import:

Specify the directory that stores the database information transferred from the migration source server. Do not change the file structure in the transferred directory. Also, do not specify the `file` option.

`file`

Specify the absolute path to the archive file of the databases transferred from the migration source server. Make sure that the absolute path does not include a space. If the database information transferred from the migration source server is stored in the directory specified by `workpath`, you do not need to specify this option.

`type`

Specify the names of the HiCommand Suite products whose databases will be migrated. Only the databases of the specified products are migrated.

You can use the `type` option to migrate the databases only when the databases of all the specified products exist in the directory specified by the archive file or the `workpath` option, and all the specified products are installed on the migration destination server. If any of the products do not meet the conditions above, migration will not be performed.

The following product names can be specified: `DeviceManager`, `GlobalLinkAvailabilityManager`, `ReplicationMonitor`, `TieredStorageManager`, and `TuningManager`. To specify multiple product names, use a comma as the delimiter between the names.

To migrate the databases of all the installed HiCommand Suite products at a time, specify `ALL`. The databases of the HiCommand Suite products installed on the migration destination server are automatically selected and migrated.

Caution: If Replication Monitor version 4.2 is installed on the migration source machine, you cannot migrate the database. We recommend that you upgrade Replication Monitor on the migration source and migration destination machines to version 5.0 or later, and then perform migration. If Replication Monitor cannot be upgraded to version 5.0 or later, or the Replication Monitor database does not have to be migrated, use the `type` option and specify all products other than Replication Monitor when you execute the command. For details on how to migrate Replication Monitor, contact Customer Support.

The following table lists the actions to be taken when an error message is output. If a message that does not have one of the following message IDs is output, take actions according to the message.

Table 4.11 Action to Be Take When an Error Message Is Output (During an Import)

Message ID	Action
KAPM05909-E	Collect maintenance information, and then contact Customer Support.
KAPM05910-E	Make sure that the products have been properly installed, and if necessary, take

	actions to satisfy this condition. If an error still occurs after taking the above actions, collect maintenance information, and then contact Customer Support.
KAPM05911-E	Check the version of the products. If migration is not supported for the version of the products, use the <code>type</code> option to import all products other than the unsupported products.
KAPM05913-E	Perform one of the following operations: - Install the products that are not installed on the migration destination. - Use the <code>type</code> option to import only the products installed on the migration destination.
KAPM05914-E	Use the <code>type</code> option to specify only the products that are included in the archive file or in the directory specified by the <code>workpath</code> option.
KAPM05915-E	Check the data to be imported.
KAPM05916-E	Check the data to be imported and the setting of the server to which the data is to be imported.
KAPM05921-E	Make sure the following conditions are satisfied, and if necessary, take actions to satisfy them: - The capacity of the disk used for the directory specified by the <code>workpath</code> option is sufficient. - The archive file is for the <code>hcmdsdbtrans</code> command. If an error still occurs after taking the above actions, collect maintenance information, and then contact Customer Support.
KAPM05926-E	- When the <code>file</code> option is specified Check whether the specified file is the archive file for the <code>hcmdsdbtrans</code> command. - When the <code>file</code> option is not specified Check whether all the contents of the directory specified by the <code>workpath</code> option while exporting are stored in the directory specified by the <code>workpath</code> option. If an error still occurs after taking the above actions, collect maintenance information, and then contact Customer Support.

4. Synchronize the repository information with the imported Device Manager database information.

Specify `true` for the `server.base.initialsynchro` property in the `server.properties` file.

Since, other than user information, the `hcmdsdbtrans` command does not migrate the HiCommand Suite Common Component repository, you need to synchronize the repository information with the database information of the imported Device Manager.

For information on the `server.base.initialsynchro` property, see section 8.2.22.

5. From the terminal window, execute the following command to restart the Device Manager server and HiCommand Suite Common Component:

```
# /opt/HiCommand/suitesrvctl -start_all
```

4.8.4 Initializing the Device Manager Server Database

To initialize the database:

1. From a terminal window, enter the following command to stop the Device Manager Server:
/opt/HiCommand/suitesrvctl -stop_hdvm
2. Verify that the server is not running.
/opt/HiCommand/suitesrvctl -status_hdvm
3. The output of this command should display several lines of text. The second line of the output should display the text **HiCommand is not running**. If instead it displays a process ID, HiCommand Device Manager is still running. Return to step 1 to stop the Device Manager Server.
4. Confirm that HiRDB is running.
/opt/HiCommand/Base/bin/hcmdssrv -status
5. This command outputs several lines of messages. If the following message is included, then HiRDB is running normally.
KAPM06440-I The HiRDB service has already started.
6. If HiRDB is not running, execute the following command:
/opt/HiCommand/Base/bin/hcmdssrv -start
7. From the command prompt, execute the database command.
/opt/HiCommand/database.sh database initialize
8. Specify **true** for the **server.base.initialsynchro** property in the server.properties file. See section 8.2.23 for more information.
9. Restart the Device Manager Server.
/opt/HiCommand/suitesrvctl -start_hdvm
10. Verify that the server is running.
/opt/HiCommand/suitesrvctl -status_hdvm
11. This command outputs several lines of text. The first line of text should read:
HiCommand process ID: xxxx. This indicates that the Device Manager Server is up and running normally.
12. In the server.properties file, change the **server.base.initialsynchro** property back to false. See section 8.2.23 for more information.

4.9 Converting a Device Manager Server Database

To use a database that has been used before the upgrade when upgrading the Device Manager server version 2.3 through 3.5 to 4.0 or later, you must first convert it to HiRDB.

Caution: The conversion function is available only when the upgrade is from the Device Manager server version 2.3 through 3.5 to Device Manager server version 4.0 or later.

4.9.1 About Converting from InterBase to HiRDB

If you have a Device Manager database for versions 2.3 through 3.5, it is based on InterBase. Databases for versions 4.0 and higher are based on HiRDB, so if you are upgrading to that level you will need to convert the database.

Caution: InterBase, InterServer and HiRDB must all be running when you convert the database.

Note: It might take a long time to convert the database. For example, if 8,000 LDEVs and 16,000 paths have been managed, the database conversion will take about 10 minutes in an environment that has a 900 MHz CPU and 2 GB of memory.

4.9.2 Converting Manually to HiRDB

You can either convert the database automatically when you install the Device Manager Server, or manually after the installation using these instructions.

To manually convert a database:

1. Stop the Device Manager Server.
/opt/HiCommand/suitesrvctl -stop_hdvm
2. Verify that the Device Manager Server is not running.
/opt/HiCommand/suitesrvctl -status_hdvm
3. This command outputs several lines of text, the second of which is **HiCommand is not running**. If a process ID is output, HiCommand Device Manager is still running. Return to step 1, and stop the Device Manager Server.
4. If InterBase and InterServer are not running, start them manually.
/etc/init.d/interbaseserver start
5. Verify that HiRDB is running.
/opt/HiCommand/Base/bin/hcmdssrv -status
6. If the following message is included in those messages, HiRDB is running normally.
KAPM06440-I The HiRDB service has already started.
7. If HiRDB is not running, start it manually.
/opt/HiCommand/Base/bin/hcmdssrv -start
8. To convert the database for the specified file, use the script file, along with the following parameters.
 - **migrateFmlB.sh [-d InterBase-GDB-file-name | InterBase-GBK-file-name] [-h host-with-InterBase-files] [-u InterBase-user-id] [-p InterBase-password]**
9. The following options can be specified for the **migrateFmlB** command.
 - **-d:** Specify an absolute path for the name of the GDB or GBK file for InterBase. The following file is used if the **-d** option is not specified:

/opt/HiCommand/HiCommandServer/database/interbase/HiCommand.gdb

- **-h:** Specify the host name or IP address of the host on which the InterBase files exist. localhost is assumed if nothing is specified.
- **-u:** Specify the InterBase user ID. The default InterBase user ID is assumed if the -u option is not specified.
- **-p:** Specify the InterBase password. The password of the default InterBase user ID is used if the -p option is not specified.

10. Specify **true** for the **server.base.initialsynchro** property in the **server.properties** file. See section 8.2.23 for more information.

11. Restart the Device Manager Server.

/opt/HiCommand/suitesrvctl -start_hdvm

12. Verify that the Device Manager Server is running.

/opt/HiCommand/suitesrvctl -status_hdvm

13. This command outputs several lines of text, the second of which is **HiCommand process ID: xxxx**. This indicates that HiCommand Device Manager is running properly.

14. In the server.properties file, change the **server.base.initialsynchro** property back to false. See section 8.2.23 for more information.

Table 4.12 lists the return codes for the migrateFmIB command

Table 4.12 Return codes for the migrateFmIB Command

Return Code	Description
0	The command terminated normally.
1	InterBase is not running.
2	HiRDB is not running.
3	An InterBase authentication error occurred.
4	A HiRDB authentication error occurred.
5 to 19	(Reserved)
20	The Device Manager Server is running.
21 to 29	(Reserved)
30	The database file to be converted does not exist.
31 to 39	(Reserved)
40	An attempt to change the database definition has failed.
41 to 49	(Reserved)
50	An attempt to convert the database has failed.
51 to 253	(Reserved)
254	An error occurred during the convert.
255	Internal error.

4.10 Uninstalling the HiCommand Device Manager Server and Related Products

Caution: You must restore the kernel parameters after uninstalling the Device Manager server. To restore the kernel parameters that have been set, see section 4.12 for Solaris, or see section 4.13 for Linux.

If the kernel parameter setting has been changed, execute **shutdown -y -i6 -g0** and then reboot the system.

4.10.1 Uninstalling Device Manager Server in a Standard Environment

Unless you are experiencing problems and need to completely re-do an installation, you should not uninstall Device Manager. If you need to uninstall the Device Manager Server, make sure to first back up your configuration (see section 4.8.1 for instructions).

WARNING: When you are using the Single Sign-On function and a HiCommand Device Manager server and HiCommand Tuning Manager are installed on the same machine, the HBase Storage Mgmt Common Service is deleted when HiCommand Device Manager is uninstalled.

Warning: Do not specify the system's zone settings during uninstallation in Solaris 10 system. If you do specify the settings, uninstallation might finish abnormally.

If no other program is using the Common Component, it will be uninstalled during the uninstallation of Device Manager. If another program is using the Common Component, it will remain installed. You cannot uninstall the Common Component by itself.

When you uninstall Device Manager, the directories or files under <installation directory> will be deleted, but the directory itself will remain after the uninstallation. If the directory is not necessary you can delete it manually.

WARNING: Files may remain in the installation directory, especially if they were added manually after installation. You can delete unnecessary files, but do not delete this directory if another HiCommand Suite product is being used.

Caution: When you uninstall HiCommand Device Manager from a computer on which another HiCommand Suite product is installed, a **GO** menu command for launching Device Manager remains on the dashboard of that program. To remove **GO**, a user with User Management permissions must execute the following command. When this command is executed, the HiCommand Suite Common Component services must be running.

```
/opt/HiCommand/Base/bin/hcmdsintg -delete -type DeviceManager -user user-ID -pass password
```

Caution: Check whether the following programs are installed. If they are installed, take action by following the explanation below:

- A program that monitors security
Stop the program that monitors security, or change its settings so that Device Manager can be uninstalled normally.
- A program that detects viruses

We recommend that you stop programs that detect viruses, and then uninstall Device Manager.

If a program that detects viruses is running during uninstallation of Device Manager, the speed of uninstallation might be reduced, uninstallation might fail, or uninstallation might finish in an incorrect state.

- A program that monitors processes

Stop the program that monitors processes, or change its settings so that the program does not monitor the processes of the HiCommand Device Manager server and the HiCommand Suite Common Component.

If a program that monitors processes starts or stops the above processes during uninstallation of Device Manager, uninstallation might fail.

Note: HiCommand Device Manager provides user management functions for the HBase Storage Mgmt Common Service. When the HiCommand Device Manager Server is uninstalled, the HBase Storage Mgmt Common Service no longer operates. Therefore, if you are using Tuning Manager installed on the same machine as the Device Manager Server, Tuning Manager will not have access to the HBase Storage Mgmt Common Service after Device Manager is uninstalled. Before you uninstall the Device Manager, you must disable use of the HBase Storage Mgmt Common Service in the Tuning Manager settings.

To uninstall the Device Manager Server:

1. Stop all other HiCommand Suite software that is running.
2. Enter the Device Manager package removal command.

Move the current directory to the root (/), and then execute the following command:

```
# /opt/HiCommand/Uninstall/uninstall.sh
```

3. A message confirming that you want to delete Device Manager Server and the Common Component is displayed. Enter **y** to begin the uninstallation.
4. When the HiCommand Suite Common Component services are running, a message is displayed to confirm whether you want these services to stop. stop (see Figure 4.32) To stop the uninstallation, select **n**. To continue the uninstallation, select **y**.

If the uninstaller cannot stop the HiCommand Suite Common Component services, a message is displayed to notify you that you need to start the uninstallation after stopping the other HiCommand Suite products, and then the uninstallation stops (see Figure 4.33).

Caution: If the following message is displayed in Linux, manually release the SLP daemon from the Linux daemon. If directories and files related to SLP remain, manually delete them as necessary. For details about how to release the SLP daemon, see section 11.5.1.3.

WARNING: An attempt to release the SLP daemon has failed. After uninstallation, release the SLP daemon manually. Uninstallation continues.

Note: Files can remain in the installation directory. Do not delete this directory if another HiCommand Suite product is being used.

Note: If no program is using the Common Component, the Common Component will be uninstalled during the uninstallation of the Device Manager Server. If one or more other programs are using the Common Component, it will be uninstalled only when you uninstall the last program that is using it.

If you uninstall the HiCommand Device Manager server from a machine where software containing HiCommand Suite Common Component has already been installed, HiCommand Suite Common Component will not be uninstalled.

```
Stop HiCommand Suite Common Component Services:
To continue processing, HiCommand Suite Common Component services will be
stopped. However, these services cannot stop if a service of another HiCommand
Suite product is running. So, before continuing, please stop the services of
all other HiCommand Suite products.

Do you want to continue uninstallation? [y/n]
```

Figure 4.32 Message that Confirms Stopping of Services (appears during uninstallation)

```
ERROR: HiCommand Suite processes are running. Perform the following operation,
and redo the uninstall process:
1. If applicable, stop other HiCommand Suite software except the Device
Manager.
2. Stop the Device Manager Server.
3. Stop HiCommand Suite Common Component. Execute the following command:
/opt/HiCommand/Base/bin/hcmdssrv -stop
```

Figure 4.33 Message Notifying that Another HiCommand Suite Product Is Running

4.10.2 Uninstalling Device Manager Server in a VERITAS Server Environment

Note: Before uninstalling, you must confirm that the services on the executing node are online. If the services are offline on the executing node, switch them online.

1. Start Cluster Manager (Java Console).
2. Place the following services offline: (See section 5.2.2 if you need instructions.)
 - HiCommand Server
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service

The above services are represented by the resource names registered in section 4.5.3.5.

3. Stop HiCommand Suite Common Component by executing the following command.
/opt/HiCommand/Base/bin/hcmdssrv -stop
4. Place the HiRDB service offline.
5. Delete the following resources, provided that no other applications are using them:
 - HBase Storage Mgmt Web Service
 - HBase Storage Agent Common Service
 - HiCommand Server
 - HiRDB

The above services are represented by the resource names registered in section 4.5.3.5.

Caution: Do not use this procedure to delete the IP address and shared disk resources.

6. For resources that you will not be deleting, right-click to display a menu, and then deselect **Enabled**.
7. In the Cluster Explorer window do the following, select the **Service Groups** tab.
8. Right-click the group to which the HiCommand Device Manager services have been registered, and choose **Freeze** and then **Temporary**.
9. Uninstall the Device Manager Server on the executing node.
Move the current directory to the root (/), and then execute the following command:
/opt/HiCommand/Uninstall/uninstall.sh
10. Manually delete the unnecessary files and directories that were created during installation in the cluster environment.
11. In the Cluster Explorer panel, do the following:
 - Select **Service Groups**.
 - Select the group to which the HiCommand Device Manager service has been registered.
 - Right-click to display a menu.
 - Choose **Unfreeze**.
 - Choose **Switch To**, and then **Host Name**.
 - Choose **Freeze**, and then **Temporary**.
12. Uninstall HiCommand Device Manager on the standby node.
Move the current directory to the root (/), and then execute the following command:
/opt/HiCommand/Uninstall/uninstall.sh
13. Manually delete the unnecessary files and directories that were created during installation in the cluster environment.
14. Delete the following resources, provided that no other applications are using them:
 - IP address
 - Shared disk
15. For the group to which the HiCommand Device Manager resources were registered, do the following:
 - If is no longer necessary, delete it.
 - If it is still necessary, in the Cluster Explorer window, select the **Service Groups** tab. Right-click the group to which the HiCommand Device Manager services have been registered, and then choose **Unfreeze**.
16. Enable the resources that you disabled in step 6.

4.10.3 Uninstalling Device Manager Server in a Sun Cluster Environment

Note: Before uninstalling, you must confirm that the services on the executing node are online. If the services are offline on the executing node, switch them online.

1. On the executing node, disable the monitoring of the resources of the HiCommand Suite Common Component and HiCommand Device Manager.

```
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
```

```
# /usr/cluster/bin/scswitch -n -M -j MgmtWebService
```

```
# /usr/cluster/bin/scswitch -n -M -j MgmtComService
```

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

For the resource names in the above commands, specify the resource names registered section 4.5.3.6.

2. Disable the following service resources.

```
# /usr/cluster/bin/scswitch -n -j HiCommandServer
```

```
# /usr/cluster/bin/scswitch -n -M -j MgmtWebService
```

```
# /usr/cluster/bin/scswitch -n -M -j MgmtComService
```

```
# /usr/cluster/bin/scswitch -n -j HiRDB.
```

For the resource names in the above commands, specify the resource names registered section 4.5.3.6.

3. Delete the following resources, provided that no other applications are using them:

- HBase Storage Management Web Service
- HBase Storage Mgmt Common Service
- HiCommand Server
- HiRDB

The above services are represented by the resource names registered in section 4.5.3.6.

Note: Do not use this procedure to delete the IP address and shared disk resources.

4. Uninstall the Device Manager Server on the executing node.

Move the current directory to the root (/), and then execute the following command:

```
# /opt/HiCommand/Uninstall/uninstall.sh
```

Note: Manually delete the unnecessary files and directories that were created during installation in the cluster environment.

5. Place the group to which the HiCommand Device Manager has been registered on standby.

```
# /usr/cluster/bin/scswitch -z -g group-name -h host-name
```

6. Uninstall HiCommand Device Manager on the standby node.

Move the current directory to the root (/), and then execute the following command:

```
# /opt/HiCommand/Uninstall/uninstall.sh
```

7. Manually delete the unnecessary files and directories that were created during installation in the cluster environment.
8. Delete the following resources, provided that no other applications are using them:
 - IP address
 - Shared disk
9. For the group to which the HiCommand Device Manager resources were registered, do the following:
 - If is no longer necessary, delete it.
 - If it is still necessary, execute the following commands for those services:


```
# /usr/cluster/bin/scswitch -e -j service-name
```

```
# /usr/cluster/bin/scswitch -e -M -j service-name
```

4.11 Uninstalling InterBase Components

Notes: You will only have InterBase Server and Client installed if you were previously using Device Manager version 3.5 or lower, or if you were using another product that has InterBase as its database. Do not uninstall InterBase Server and Client if another product is using them.

4.11.1 Uninstalling InterBase Server

Note: When an InterBase process is running, you cannot uninstall InterBase. You can end an InterBase process using one of in the following methods:

- If an **/etc/init.d/interbaseserver** file exists, type the following command:


```
# /etc/init.d/interbaseserver stop
```
- If no **/etc/init.d/interbaseserver** file exists, type the following command:


```
# kill -TERM `ps -ef | grep ibserver | grep -v grep | awk '{print $2}'`
```

To uninstall InterBase:

1. Log on as the root user.
2. Stop InterBase by using one of the following methods:
 - If Device Manager is already installed:


```
# /etc/init.d/interbaseserver stop
```
 - If Device Manager is not already installed:


```
# kill -TERM `ps -ef | grep ibserver | grep -v grep | awk '{print $2}'`
```
3. Enter the command:


```
# pkgrm IBCSN60
```
4. Answer **y** to the verification prompts.

Note: A directory structure may have been left on disk as a result of the InterBase installation log file that is generated. Enter the following command to remove this directory:

```
# rm -rf /opt/interbase
```

5. Delete the following links and file manually:

- **/etc/rc2.d/K99interbaseserver**
- **/etc/rc3.d/S98interbaseserver**
- **/etc/init.d/interbaseserver**

4.11.2 Uninstalling InterClient

Note: You will only have InterClient installed if you were previously using Device Manager version 3.5 or lower, or if you were using another product that has InterBase as its database. Do not uninstall InterClient if another product is using them.

To uninstall the InterClient software:

1. Enter the following command:

```
rm -rf /usr/interclient
```

Note: If /usr/interclient is a link, then you also need to delete its linked directory.

2. Delete the entry for the InterServer software in the /etc/services file (for example, **interserver 3060/tcp**).
3. Delete the entry for the InterServer software in the **/etc/ometa/conf** file.
4. Either reboot the system, or force the inetd daemon to re-read its configuration file by entering the following command:

```
# kill -HUP `ps -ef | grep initd | grep -v grep | awk '{print $2}'`
```

4.12 Setting Kernel Parameters on Solaris

Before installing the Device Manager server, you must set the OS parameters (kernel parameters). If the kernel parameters have not been set correctly, installation fails.

When you uninstall the Device Manager server, you must change the kernel parameters back to the previous settings specified before the installation of the Device Manager server.

4.12.1 When No Other HiCommand Suite Product (version 4.0 or later) is Installed

The following describes the procedure for setting the kernel parameters in a Solaris environment.

Before changing kernel parameter settings, save the current kernel parameter settings by following the instructions for the version of your OS as shown below. After uninstalling the Device Manager server, you can use the saved settings to restore the previous kernel parameter settings.

For Solaris 8 or Solaris 9:

Create a backup of the `/etc/system` file.

For Solaris 10:

Check the current settings by using a command such as `prctl`, and then record the settings. (For details about how to check the settings, see the manuals for the OS.)

Table 4.13 or Table 4.14 below lists the recommended values for the kernel parameters you must set.

Refer to Table 4.13 or Table 4.14, and then set the kernel parameters according to the following formula (in the formula, "Max {x, y, z}" means using the maximum value among x, y, and z).

- Parameters other than `shmsys:shminfo_shmmax` for Solaris 8 or Solaris 9, or parameters other than `project.max-shm-memory` for Solaris 10:
setting-value-of-the-kernel-parameter =
Max {*currently-set-value-for-the-kernel-parameter*^{#1}, recommended-value-for-HiCommand-Suite-Common-Component + recommended-value-for-Device-Manager-server, recommended-value-for-HiRDB}
- `shmsys:shminfo_shmmax` (for Solaris 8 or Solaris 9):
setting-value-of-the-kernel-parameter =
Max {*currently-set-value-for-the-kernel-parameter*^{#1}, recommended-value-for-HiCommand-Suite-Common-Component + recommended-value-for-Device-Manager-server, recommended-value-for-HiRDB}
- `project.max-shm-memory` (for Solaris 10):
setting-value-of-the-kernel-parameter =
value-already-used-for-operation^{#2} + recommended-value-for-HiCommand-Suite-Common-Component + recommended-value-for-Device-Manager-server + recommended-value-for-HiRDB

#1: A user specified value or an initial value of the OS

#2: Total amount of shared memory that is used by the applications other than Device Manager running on the machine on which the server is installed

Caution: In Solaris 10, specify the kernel parameters for both the `user.root` project and the system project.

Caution: The maximum value of each kernel parameter must not exceed the value defined for the OS.

Caution: After changing the kernel parameters, execute the `shutdown -y -i6 -g0` command to restart the system.

The installer of the Device Manager server checks each kernel parameter by referring to the installer checking values listed in Table 4.13 or Table 4.14. If the specified value of a kernel parameter is less than the corresponding installer checking value, installation fails.

Table 4.13 Recommended values for kernel parameters (for Solaris 8 or Solaris 9)

Kernel parameter	Recommended value for HiRDB	Recommended value for HiCommand Suite Common Component	Recommended value for the Device Manager server	Installer checking value
<code>msgsys:msginfo_msgmni</code>	0	32	0	82
<code>msgsys:msginfo_msgtql</code>	0	480	0	520
<code>semsys:seminfo_semmni</code>	1024	9	1	1024
<code>semsys:seminfo_semmns</code>	7200	80	44	7200
<code>semsys:seminfo_semmnu</code>	1024	0	0	1024
<code>semsys:seminfo_semmume</code>	512	0	0	512
<code>semsys:seminfo_semmsl</code>	128	0	0	128
<code>semsys:seminfo_sempm</code>	128	0	0	128
<code>shmsys:shminfo_shmmax</code>	200000000	11542528	130000000	200000000
<code>shmsys:shminfo_shmmni</code>	2000	0	0	2000
<code>shmsys:shminfo_shmseg#</code>	240	0	0	240

In Solaris 9, the setting of this kernel parameter is not necessary. This parameter remains only when checking for compatibility with Solaris 8 (installer checking is performed only when Solaris 8 is used).

Table 4.14 Recommended values for kernel parameters (for Solaris 10)

Kernel parameter	Recommended value for HiRDB	Recommended value for HiCommand Suite Common Component	Recommended value for the Device Manager server	Installer checking value
<code>process.max-msg-messages</code>	0	480	0	8192
<code>process.max-sem-nsems</code>	128	0	0	512
<code>process.max-sem-ops</code>	128	0	0	512

Kernel parameter	Recommended value for HIRDB	Recommended value for HiCommand Suite Common Component	Recommended value for the Device Manager server	Installer checking value
<code>project.max-msg-ids</code>	0	32	0	128
<code>project.max-sem-ids</code>	1024	9	1	1024
<code>project.max-shm-ids</code>	2000	0	0	2000
<code>project.max-shm-memory</code>	0	26214400	235929600	262144000

4.12.2 When Another HiCommand Suite Product (version 4.0 or later) is Installed

If another HiCommand Suite product (version 4.0 or later) is already installed, the kernel parameter values recommended for that product are required.

For each kernel parameter, set the sum of the recommended values for the HiCommand Suite Common Component, Device Manager server, and the existing HiCommand Suite product.

For the recommended values for the HiCommand Suite product, see the appropriate product manual or Release Notes.

Caution: In Solaris 10, specify the kernel parameters for both the `user.root` project and the system project.

Caution: After changing the kernel parameters, execute the `shutdown -y -i6 -g0` command to restart the system.

4.12.3 Setup Needed After Uninstallation of the Device Manager Server

If kernel parameters were already set when you installed the Device Manager server, restore them to their previous settings by following the instructions for the version of your OS as shown below:

For Solaris 8 or Solaris 9:

Replace the current file with the `/etc/system` file that you backed up.

For Solaris 10:

Set the recorded settings. (For details about how to do this, see the manuals of the OS.)

If kernel parameters were not set, and you did not back up the above file, restore the settings to the initial values for the OS.

Caution: After changing the kernel parameters, execute the `shutdown -y -i6 -g0` command to restart the system.

4.13 Setting Kernel Parameters and Shell Restrictions on Linux

Before installing the Device Manager server, you must set the OS parameters (kernel parameters and shell restrictions). If the kernel parameters have not been set correctly, installation fails.

When you uninstall the Device Manager server, you must change the kernel parameters and shell restrictions back to the previous settings specified before the installation of the Device Manager server.

The following describes the procedure for setting the kernel parameters and shell restrictions in a Linux environment.

Before changing kernel parameter settings and shell restrictions, back up the `/etc/sysctl.conf` file and `/etc/security/limits.conf` file. You can use the backup files to restore the previous kernel parameter settings and shell restrictions after you uninstall the Device Manager server.

Table 4.15 below shows the recommended values for the shell restrictions and Table 4.16 shows the recommended values for the kernel parameters you must set.

Refer to these two tables, to set the shell restrictions and kernel parameters according to the following formula (in the formula, "Max {x, y, z}" means using the maximum value among x, y, and z).

- `kernel.shmmax`:
setting-value-of-the-kernel-parameter =
 $\text{Max \{currently-set-value-for-the-kernel-parameter}^\#, \text{recommended-value-for-HiCommand-Suite-Common-Component} + \text{recommended-value-for-the-Device-Manager-server}, \text{recommended-value-for-HiRDB}\}$
- `kernel.shmall`:
setting-value-of-the-kernel-parameter =
 $\text{currently-set-value-for-the-kernel-parameter}^\# + \text{recommended-value-for-HiCommand-Suite-Common-Component} + \text{recommended-value-for-the-Device-Manager-server} + \text{recommended-value-for-HiRDB}$
- All other kernel parameters and shell restrictions:
setting-value-of-the-shell-restriction-or-kernel-parameter =
 $\text{Max \{currently-set-value-for-the-kernel-parameter}^\# + \text{recommended-value-for-HiCommand-Suite-Common-Component} + \text{recommended-value-for-the-Device-Manager-server}, \text{recommended-value-for-HiRDB}\}$

#: A user specified value or an initial value of the OS

Caution: The setting value of each kernel parameter and shell restriction must not exceed the maximum value defined for the OS.

Caution: Set the shell restrictions for both `soft` and `hard`. At this time, you must set the value for `soft` to a value that is smaller than the value for `hard`.

Caution: After changing the kernel parameters or shell restrictions, execute the `reboot` command to restart the system.

The installer of the Device Manager server checks each kernel parameter and shell restriction by referring to the installer checking values listed in the table below. If a specified value is less than the corresponding installer checking value, installation fails.

Table 4.15 Recommended Values for Shell Restrictions (`/etc/security/limits.conf`)

Shell restriction	Recommended value for HiRDB	Recommended value for HiCommand Suite Common Component	Recommended value for the Device Manager server	Installer checking value
<code>nofile</code> (soft/hard)	1344	572	0	1596
<code>nproc</code> (soft/hard)	512	165	1	5862

An example of setting shell restrictions is shown below.

#<domain>	<type>	<item>	<value>
#			
*	soft	nofile	1596
*	hard	nofile	1596
*	soft	nproc	5862
*	hard	nproc	5862

Table 4.16 Recommended Values for Kernel Parameters (`/etc/sysctl.conf`)

Kernel parameter	Recommended value for HiRDB	Recommended value for HiCommand Suite Common Component	Recommended value for the Device Manager server	Installer checking value
<code>fs.file-max</code>	53898	53898	1075	90150
<code>kernel.threads-max</code>	576	184	20	11596
<code>kernel.msgmni</code>	32	32	0	48
<code>kernel.sem</code> (4 th parameter)	1024	9	1	1024
<code>kernel.sem</code> (2nd parameter)	7200	80	44	32124
<code>kernel.shmmax</code>	200000000	11542528	74022920	200000000
<code>kernel.shmmni</code>	2000	0	0	4096
<code>kernel.shmall</code>	22418432	22418432	79520488	126454504

4.13.1 Setup Needed After Uninstallation of the Device Manager Server

If kernel parameters and shell restrictions were already set when you installed the Device Manager server, restore them to their previous settings from the following files that you backed up before installation.

- `/etc/sysctl.conf`
- `/etc/security/limits.conf`

If kernel parameters and shell restrictions were not set, and you did not back up the above files, change the settings to the initial values of the OS.

Caution: After changing the kernel parameters or shell restrictions, execute the `reboot` command to restart the system.

Chapter 5 Using the HiCommand Suite Common Component

The HiCommand Suite Common Component provides features that are used by all HiCommand Suite products. Each HiCommand Suite product will bundle the Common Component.

This chapter discusses the following functions:

- Installing and Uninstalling the Common Component (see section 5.1)
- Starting and Stopping the Common Component (see section 5.2)
- Integrated Logging (see section 5.3)
- Ports Used By the Common Component (see section 5.4)
- Setup for Starting a Web Application From Web Client (see section 5.5)
- Changing the Host Name of the Management Server (see section 5.6)
- Security Settings for User Accounts (see section 5.7)
- Warning banner settings (see section 5.8)

5.1 Installing and Uninstalling HiCommand Suite Common Component

The Common Component must be installed or uninstalled as part of the installation or uninstallation of another HiCommand product, e.g., Device Manager or Tuning Manager. You cannot install or uninstall just the Common Component.

Installation of the Common Component will include the Hitachi Network Objectplaza trace common library.

Whether the Common Component is either installed or upgraded during Device Manager installation is determined by following factors:

- If the Common Component is not previously installed on the system, the Device Manager installer will install it.
- If the previously installed Common Component version is older than or equal to the installing Common Component version, the Device Manager installer will upgrade the Common Component by overwriting the previous installation.
- If the previously installed Common Component version is newer than the installing Common Component version, the previously installed version is left intact.

Whether the Common Component is uninstalled or left in place during Device Manager uninstallation is determined by the following factors:

- If any other HiCommand Suite products are using the Common Component, the Common Component will not be uninstalled. The Common Component will not be uninstalled until the last HiCommand Suite product that uses the Common Component is uninstalled.

- If the Common Component is being used by only by Device Manager, it will be uninstalled as part of the Device Manager uninstallation process.

Table 5.1 describes the Common Component elements that are used by Device Manager.

Table 5.1 Device Manager Common Component Elements

Function	Description
HBase Storage Mgmt Common Service	A customer who operates multiple HiCommand Suite products is not prompted to re-enter their user ID and password if that customer is using those products simultaneously. HBase Storage Mgmt Common Service provides a unified user authentication mechanism.
Integrated logging information	Operation and other types of logs are concentrated by an integrated logging information feature. Providing a common log repository allows all HiCommand Suite log files to be in the same file.

5.2 Starting and Stopping HiCommand Suite Common Component

5.2.1 Starting the Common Component

Ordinarily you should not need to manually start the Common Component.

To start HiCommand Suite Common Component, start the following services:

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB

To start the Common Component in a Windows environment:

1. Log in to the system as a user with Administrator privileges.
2. Start the Common Component.

<common component installation folder>\bin\hcmdssrv /start

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /start

3. Verify that the Common Component has started.

<common component installation folder>\bin\hcmdssrv /status

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /status

4. If the following messages appear, the services are running:

KAPM06440-I The HiRDB service has already started.

KAPM05007-I Already started service. service-name=HBase Storage Mgmt Web Service

KAPM05007-I Already started service. service-name=HBase Storage Mgmt Common Service

To start the HiCommand Suite Common Component in a Solaris or Linux environment:

1. Log in to the system as root.
2. Start the Common Component.
/opt/HiCommand/Base/bin/hcmdssrv -start
3. Verify that the Common Component has started.
/opt/HiCommand/Base/bin/hcmdssrv -status
4. If the following messages appear, the services are running:

KAPM06440-I The HiRDB service has already started.

KAPM05007-I Already started service. service-name=HBase Storage Mgmt Web Service

KAPM05007-I Already started service. service-name=HBase Storage Mgmt Common Service

5.2.2 Stopping the Common Component

To stop HiCommand Suite Common Component, stop the following services:

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB

Note: If the Common Component is forcibly stopped in a VERITAS Cluster Server environment, certain temporary files will not be deleted. If these files are on the standby node, a message will be output to the VERITAS Cluster Server log indicating that the Common Component cannot be placed offline. You can safely ignore this message. To prevent the message from appearing in the future, do the following:

1. Verify that the Common Component is not running.
/opt/HiCommand/Base/bin/hcmdssrv -status
2. Delete **HiCommand.pid** from the /var/opt/HiCommand/Base/tmp directory.
3. Delete **httpd.pid** from the /var/opt/HiCommand/Base/httpsd/logs directory.

To stop the Common Component in a Windows environment:

1. Log on as an administrator.
2. Stop the Common Component using the following command:
<common component installation folder>\bin\hcmdssrv /stop

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

3. Verify that the Common Component has stopped.

<common component installation folder>\bin\hcmdssrv /status

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /status

4. If the following messages appear, the services have stopped:
 - **KAPM06441-I The HiRDB service has already stopped.**
 - **KAPM05009-I Already stopped service. service-name=HBase Storage Mgmt Web Service.**
 - **KAPM05009-I Already stopped service. service-name= HBase Storage Mgmt Common Service.**

To stop Common Component in a Solaris or Linux environment:

Caution: When stopping HiCommand Suite Common Component in a Solaris or Linux environment, do not execute the stop command (`hcmdssrv -stop`) before HiCommand Suite Common Component has completed startup. Regardless of whether a resident process for the service is running, the service status displayed by the `status` option might be `not running`, and the service might be unable to be stopped by the `stop` option. In such cases, reboot the system.

1. Log in to the system as root.
2. Stop the Common Component.
/opt/HiCommand/Base/bin/hcmdssrv -stop
3. Verify that the Common Component has stopped.
/opt/HiCommand/Base/bin/hcmdssrv -status
4. If the following messages appear, the services have stopped:

KAPM06441-I The HiRDB service has already stopped

KAPM05009-I Already stopped service. service-name=HBase Storage Mgmt Web Service

KAPM05009-I Already stopped service. service-name=HBase Storage Mgmt Common Service

5.3 Integrated Logging

5.3.1 Integrated Log Output

The Common Component provides common log files and a common library for log output for each program product in the HiCommand Suite. Device Manager uses this information to show the details for the log files.

Table 5.2 Integrated Log Output

Log Type	Log Name	Description	Location (Windows)	Location (Solaris, Linux)
Common trace log file	hntr2*.log	Integrated trace log information produced by the Common Component. The asterisk (*) in the file name indicates a file number.	C:\Program Files\Hitachi\HNTRLib2\spool	/var/opt/hitachi/HNTRLib2/spool
Event log/syslog file	Eventlog	Windows event log	Event viewer	N/A
	syslog	Solaris or Linux system log	N/A	Defined by /etc/syslog.co
Device Manager log file	version	Version information about the operating environment of the Device Manager Server (Device Manager Server, Java VM, and operating system)	<installation directory>\HiCommandServer\logs	/opt/HiCommand/HiCommandServer/logs
Device Manager trace log file (Common Component)	HDvMtrace*.log	Trace log information output by the Common Component and used by the Device Manager Server. The asterisk (*) in the file name indicates a file number.	<installation directory>\HiCommandServer\logs	/opt/HiCommand/HiCommandServer/logs

5.3.2 Common Component Trace Log Properties

WARNING: Changing the common trace log settings affects other program products that use the common trace log.

You can specify the number of trace log files up to a maximum of 16 (see sections 5.3.2.2). Larger numbers of trace log files can make it more difficult to find specific information.

You can also specify the size of each Common Component trace log file, from 8 KB to 4 MB (4096 KB) (see sections 5.3.2.2). The Common Component trace log monitoring program switches to the next file when the current output file reaches the specified size.

Note: The value should be larger than the value that you have set in the buffer.

5.3.2.1 Specifying the Number of Trace Log Files (Windows)

The Windows **HNTRLib2** utility is located as follows:

C:\Program Files\Hitachi\HNTRLib2\bin\hntr2util.exe

To specify the number of trace log files:

1. Log in to the system as a user with **administrator** privileges.
2. Execute hntr2util.exe.

The Hitachi Network Objectplaza Trace Utility 2 panel is displayed.

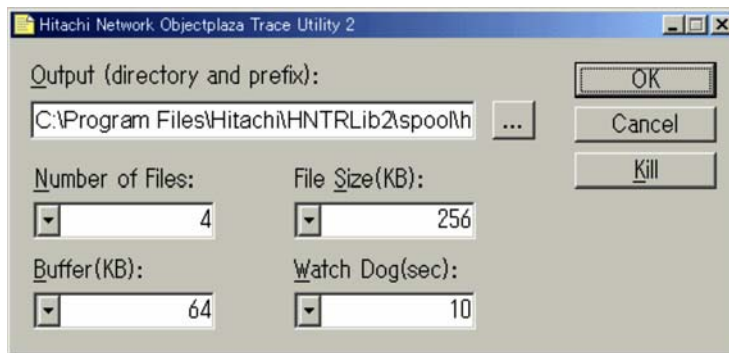


Figure 5.1 Hitachi Network Objectplaza Trace Utility 2 Panel

3. Type the desired number of trace log files, and then select **OK**.

5.3.2.2 Specifying the Size of Trace Log Files (Windows)

The Windows **HNTRLib2** utility is stored on the following path:

C:\Program Files\Hitachi\HNTRLib2\bin\hntr2util.exe

To change the size of the trace log files:

1. Log in to the system as a user with Administrator privileges.
2. Execute hntr2util.exe.

The Hitachi Network Objectplaza Trace Utility 2 panel is displayed (see Figure 5.2).

3. Type the desired size for the trace log files, and then select OK.

5.3.2.3 Specifying the Number of Trace Log Files (Solaris or Linux)

Solaris or Linux:

The utility program is stored in the following path:

/opt/hitachi/HNTRLib2/bin/hntr2util

1. Log in to the system as root.
2. Execute `hntr2util`.
A menu appears.
3. From the menu, select **Number of log files**.

The submenu appears.

```
Hitachi Network Objectplaza Trace Library 2 - Configuration Utility Rel 1.0
Type the number of files [1-16] (Type '!' to return)

Current Number: 4
New Number:
```

4. In the submenu, enter the desired number for trace log files, and then press **Enter**. If you do not want to change the number, enter `!`, and then press **Enter**.
5. Check the contents you specified, enter `e`, and then press **Enter**.
A message appears to check if you want to save the changes.
6. Enter `y` to save your changes or enter `n` to exit without saving your changes.

5.3.2.4 Selecting the Size of Trace Log Files (Solaris and Linux)

Solaris or Linux:

The utility program is stored in the following path:

`/opt/hitachi/HNTRLib2/bin/hntr2util`

To change the size of the trace log files:

1. Log in to the system as root.
2. Execute `hntr2util`.
A menu appears.
3. From the menu, select **Size of a log file**.

The submenu appears.

```
Hitachi Network Objectplaza Trace Library 2 - Configuration Utility Rel 1.0
Type new file size [8-4096] (Type '!' to return)

Current Size(KB): 256
New Size(KB):
```

4. In the submenu, enter the desired size for the trace log files, and then press **Enter**. If you do not want to change the size, enter `!`, and then press **Enter**.
5. Check the contents you specified, enter `e`, and then press **Enter**.
A message appears to check if you want to save the changes.
6. Enter `y` to save your changes or enter `n` to exit without saving your changes.

5.4 Ports Used By HiCommand Suite Common Component

5.4.1 Ports Used by Device Manager Server and Common Component

Table 5.3 lists the ports used by the Device Manager Server and the Common Component.

Table 5.3 Device Manager Server and Common Component Ports

Component	Network Port	Description
Device Manager Server	2001/tcp	Used by the Device Manager HTTP (web) Server to communicate with the Web Client and the Device Manager Agent. You can change the port using the <code>server.http.port</code> property. For details, see section 8.2.2.
	snmptrap:162/udp	Used for receiving SNMP traps from the subsystem(s).
	2443/tcp	Used by the Device Manager Server to use SSL-based communication with the CLI, the Web Client, and the Device Manager Agent. You can change this port by modifying the <code>server.https.port</code> property. For details, see section 8.2.3.
Device Manager agent	24041/tcp	Used for the Device Manager Agent HTTP (web) Server. You can change the port using the <code>server.http.port</code> property. For details, see section 8.2.2.
	24042/tcp	Used for communication between Device Manager Agent's daemon process and the web Server process. You can change this port by modifying the <code>server.http.localPort</code> property file.
	24043/tcp	Used for Device Manager Agent's daemon process (or service). You can change the port using the <code>server.agent.port</code> property.
HiCommand Suite Common Component	23015/tcp	Used by the Device Manager server to access non-SSL HBase Storage Mgmt Web Service.
	23016/tcp	Used by web browsers to access SSL HBase Storage Mgmt Web Service. If you want to change this port number after installation, see section 5.4.2. (Device Manager does not use this port).
	23017/tcp	Used by the HBase Storage Mgmt Web Service to access HBase Storage Mgmt Common Service through an AJP connection. If you want to change this port number after installation, see section 5.4.2.
	23018/tcp	Used by HBase Storage Mgmt Common Service and to receive a stop request. If you want to change this port number after installation, see section 5.4.2.
	23032/tcp	Used by HiRDB. If you want to change this port number after installation, see section 5.4.2.
	From 23019/tcp to 23031/tcp, 23033/tcp, and 23034/tcp	Reserved port
	45001/tcp	49000/tcp Used by HiRDB internal communication. Do not use these ports.

Note: If you update the database used by the Device Manager server (version 2.3 to version 3.5) to a database that can be used by the Device Manager server version 4.0, use the port numbers of gds_db:3050/tcp and interserver:3060/tcp.

5.4.2 Changing Ports Used by Common Component

After installing Device Manager, if you want to change the any of the ports used by the Common Component, use the following procedure:

1. Stop any other HiCommand Suite product that is running.
2. Stop the Device Manager Server and Common Component.

For Windows:

Select **Start, Program, HiCommand, Device Manager**, and then **Stop Server with Common Services**.

Solaris or Linux:

```
# /opt/HiCommand/suitesrvctl -stop_all
```

3. Edit the setup file, and change the port number. For details about each port's setup file, see sections 5.4.2.1 to 5.4.2.5.
4. Start the Device Manager Server and Common Component

For Windows:

Select **Start, Program, HiCommand, Device Manager**, and then **Start Server with Common Services**.

Solaris or Linux:

```
# /opt/HiCommand/suitesrvctl -start_all
```

5.4.2.1 23015/tcp (For Accessing Non-SSL HBase Storage Mgmt Web Service)

To change the port used for accessing the non-SSL HBase Storage Mgmt Web Service, you must change the port number written in the following file:

Windows:

- The listen directive in
<common component installation folder>\httpsd\conf\httpsd.conf

AND

- The port number coded in the listen directive in
<common component installation folder>\conf\hssso.conf

Solaris or Linux:

- The listen directive in
/opt/HiCommand/Base/httpsd/conf/httpsd.conf

and:

- hssso.hostport in
/opt/HiCommand/Base/conf/hssso.conf

5.4.2.2 23016/tcp (For Accessing SSL HBase Storage Mgmt Web Service)

To change the port used for accessing SSL HBase Storage Mgmt Web Service, you must change the port number written in the following files:

Windows:

- <VirtualHost host name>:port number in
<common component installation directory>\httpsd\conf\httpsd.conf
- The port number described in the listen directive in
<common component installation directory>\httpsd\conf\httpsd.conf

AND

- hssso.sslport in
<common component installation folder>\conf\hssso.conf

Solaris or Linux:

- <VirtualHost host name>:port number in
/opt/HiCommand/Base/httpsd/conf/httpsd.conf
- The port number described in the listen directive
/opt/HiCommand/Base/httpsd/conf/httpsd.conf

AND

- hssso.sslport in

5.4.2.3 /opt/HiCommand/Base/conf/hssso.conf23017/tcp (For HBase Storage Mgmt Common Service Through AJP Connection)

To change the port used for the HBase Storage Mgmt Common Service through an AJP connection, you must change the port number written in the following files:

Windows:

- worker.worker1.port in
<common component installation directory>\cc\web\redirector\workers.properties

AND

- webserver.connector.ajp13.port in
<common component installation directory>\cc\web\containers\HiCommand\usrconf\userconf.properties

Solaris or Linux:

- worker.worker1.port in
/opt/HiCommand/Base/CC/web/redirector/workers.properties

AND

- webserver.connector.ajp13.port in
**/opt/HiCommand/Base/CC/web/containers/HiCommand/usrconf/
usrconf.properties**

5.4.2.4 23018/tcp (Used for Stop Requests to HBase Storage Mgmt Common Service)

To change the port through which the HBase Storage Mgmt Common Service Service receives a stop request, you must change the port number written in the following file:

Windows:

- webserver.shutdown.port in
**<common component installation
directory>\cc\web\containers\HiCommand\usrconf\userconf.properties**

Solaris or Linux:

- webserver.shutdown.port in
**/opt/HiCommand/Base/CC/web/containers/HiCommand/usrconf/
usrconf.properties**

5.4.2.5 23032/tcp (Used for HiRDB)

To change the port used by HiRDB, you must change the port number written in the following file:

Windows:

- PDNAMEPORT in
<common component installation folder>\HDB\CONF\emb\HiRDB.ini
- pd_name_port in
<common component installation folder>\HDB\CONF\pdsys

AND

- pd_name_port in
<common component installation folder>\database\work\def_pdsys

Solaris or Linux:

- PDNAMEPORT in
/opt/HiCommand/Base/HDB/conf/emb/HiRDB.ini
- pd_name_port in
/opt/HiCommand/Base/HDB/conf/pdsys

```
AND
- pd_name_port in
  /opt/HiCommand/Base/database/work/def_pdsys
```


5.5 Setup for Starting a Web Application from Web Client

5.5.1 Using hcmdslink to Register an Application

When you choose **Go** and then **Links** in the global tasks bar area of Web Client a dialog box is displayed with links for starting applications for which the user is registered. By registering the Web applications that you often use or the information that you want to reference (such as a device installation chart) to this window, you can easily call a desired application from Web Client. To register a desired application or cancel the registration, you use the **hcmdslink** command. This section describes how to use the **hcmdslink** command.

Format:

In Windows:

```
<common component installation folder>\bin\hcmdslink {/add | /delete } /file user-defined-application-file[/nolog] /user user-identifier /pass password
```

In Solaris or Linux:

```
/opt/HiCommand/Base/bin/hcmdslink {-add | -delete } -file user-defined-application-file-name[-nolog] -user user-identifier -pass password
```

Function:

The **hcmdlink** command registers a Web application to allow you to start the desired application from Web Client, or cancels the registration.

In the user-defined application file, you specify a desired application name, URL, and name to be displayed. Then, use the **hcmdslink** command to register that information. The link to the registered application will be displayed in the link dialog box that appears when you choose **Go** and then **Links** in the global tasks bar area of Web Client.

Note: Once you register a link for starting an application, do not delete the user-defined application file used in the **hcmdslink** command. If you do, you cannot delete the link for the registered application.

Options:

add: Registers an application.

delete: Deletes an application.

file: Specifies the name of the user-defined application file. In Solaris or Linux, do not specify a path that includes a space.

user: Specifies a user ID used to register or delete the user-defined application link. Specify the user ID of a user who has the Admin permission.

pass: Specifies the password for the user ID used to register or delete the user-defined application link.

nolog: Suppresses outputting messages to the command line. However, even when this option is specified, messages for option errors are displayed.

User-defined application file:

The following shows a coding example in the user-defined application file:

Caution: To code the user-defined application file, use ASCII code only. Also note that you cannot use the control code other than the CR and LF control code.

```
@TOOL-LINK
@NAME SampleApp
@URL http://SampleApp/index.html
@DISPLAYNAME SampleApplication
@DISPLAYORDER 1
@ICONURL http://SampleApp/graphic/icon.gif
@TOOL-END
```

The items to be specified in the user-defined application file are as follows:

@TOOL-LINK: The start key. The information between the start key and the end key is the setting information. This item is required.

@NAME: Information used as the key for registration. Specify a unique name. This item is required. The maximum length of the name is 256 bytes. Use alphanumeric characters only.

@URL: The URL of the target of the link from Web Client. The maximum length of the URL is 256 bytes.

@DISPLAYNAME: The name displayed in the link dialog box that appears when you choose **Go** and then **Links** in the global tasks bar area of Web Client. If no information is specified, the name specified in @NAME is displayed. The maximum length of the name is 60 bytes.

@DISPLAYORDER: The order of the applications displayed in the link dialog box that appears when you choose **Go** and then **Links** in the global tasks bar area of Web Client. The applications are displayed in ascending order of this value. You can specify a value in the range from -2147483648 to 2147483647.

@ICONURL: The URL of the icon displayed beside the link. The maximum length of the URL is 256 bytes.

@TOOL-END: The end key. This item is required.

Return values:

- 0: Normal termination
- 255: Failure

If you do not specify the -nolog option, you can judge whether or not the command was successful from the output message. If you specify the -nolog option, no message is output. Therefore, you need to use the return value of the command to judge whether or not the command was successful. For details about errors, see the contents of the log file (hcmdslink[n].log).

Command execution examples:

When adding a link for an application:

```
C:\Program Files\HiCommand\Base\bin\hcmdslink /add /file C:\SampleLink.txt /user  
system /pass manager
```

When deleting a link for an application:

```
C:\Program Files\HiCommand\Base\bin\hcmdslink /delete /file C:\SampleLink.txt  
/user system /pass manager
```

5.5.2 Modifying the URL Information for Starting Web Client

Important: If your Device Manager Server at the recovery site has a different IP address, and you need to switch to that site, then you must change the URL pointers as described in this section. The URL must be fully qualified, e.g.,
`http://192.168.1.100:23015<http://192.168.1.100:23015/>`

Once you begin to operate Device Manager, if any of the following changes are made in the configuration, you need to modify the access information (URL information) used to start Web Client:

- Change to the IP address of a host in which the Device Manager Server is installed
- Change to a port used by HBase Storage Mgmt Web Service
- Change to the setting of the Device Manager system in order to use or stop using SSL
- Change to a remote server (for example, in the case of a remote site for disaster recovery)

The access information is stored in the database of Common Component.

To modify information stored in the database, use the `hcmdschgurl` command described below.

Format:

In Windows:

```
<common component installation folder>\bin\hcmdschgurl {/print | /change old-URL  
new-URL }
```

In Solaris or Linux:

```
/opt/HiCommand/Base/bin/hcmdschgurl {-print | -change old-URL new-URL }
```

Function:

The `hcmdschgurl` command updates the access information (URL information) used to start each application. The access information is stored in the database of Common Component.

Options:

`print`: Displays a list of URLs and programs that are currently set up

change: Overwrites the information about the currently registered URL with the information about the new URL. Specify the currently registered URL and the new URL. The specified URL must be a complete URL that contains protocols and port number.

Return values:

- 1: Argument error
- 2: URL does not exist
- 253: Restoration failure
- 254: Backup failure
- 255: Abnormal termination

For details about the errors, see the contents of the log file (HcmdsChangeURL[n].log).

Command execution example:

The following shows examples of the hcmdschgurl command execution.

1. First, execute the command with specifying the print option to find the URL information registered in the current database.
2. Next, execute the command with specifying the change option to update the URL information. In the following example, the URL information `http://192.168.11.33:23015` is changed to <http://192.168.11.55:23015>.
3. Finally, execute the command with specifying the print option to confirm the results.

```
> C:\Program Files\HiCommand\Base\bin\hcmdschgurl /print
http://192.168.11.33:23015 DeviceManager
```

```
> C:\Program Files\HiCommand\Base\bin\hcmdschgurl /change
http://192.168.11.33:23015
http://192.168.11.55:23015
```

The URL was changed from "http://192.168.11.33:23015" to "http://192.168.11.55:23015".

```
> C:\Program Files\HiCommand\Base\bin\hcmdschgurl /print
http://192.168.11.55:23015 DeviceManager
```

5.6 Changing the Host Name of the Management Server

To change the host name for the management server on which the Device Manager server is installed, you must edit several settings files beforehand.

Caution: If you change the host name of the management server before you change the host name in the Device Manager settings file, use the `hostname` command to display and write down the changed host name (for Windows, the `ipconfig /ALL` command can also be used to display host names). For the host name in the Device Manager settings file, specify the name you recorded earlier. Note that this name is case-sensitive.

To edit the settings files:

1. Stop any other HiCommand suite product that is running.
2. Stop the Device Manager server and HiCommand suite Common Component.

For Windows:

Choose **Start, Program, HiCommand, Device Manager**, and then **Stop Server with Common Services**

For Solaris or Linux:

Execute the following command:

/opt/HiCommand/suitesrvctl -stop_all

3. If the SSL settings have been configured, configure them again.

Use the host name after the change to configure the SSL settings. For details on how to configure SSL settings, see section Chapter 7.

4. Edit the `httpsd.conf` file.

Change the value for the `ServerName` parameter to the host name after the change.

The following describes the storage destination for the `httpsd.conf` file.

For Windows:

installation-folder-for-HiCommand-Suite-Common-Component\httpsd\conf

For Solaris or Linux:

/opt/HiCommand/Base/httpsd/conf/

If SSL is set, you must also do the following:

- Change the host name specified for the `<VirtualHost>` tag to the host name after the change.
- Change the value for the `ServerName` parameter in the `<VirtualHost>` tag to the host name after the change.

Important: Proceed to the next step according to the following cases:

- For a cluster configuration:

Proceed to step 5.

- For a non-cluster configuration:

If you performed a new installation of version 5.0 or later, or performed a new installation of version 5.0 or later and then performed a re-installation, skip to step 9. In other cases, proceed to step 5.

5. Edit the `pdsys` file and `def_pdsys` file.

Change the value for the `-x` option for the `pdunit` parameter to the loopback address `127.0.0.1`.

Note: Specify a virtual host name for a cluster configuration.

The following describes the storage destinations for the `pdsys` file and `def_pdsys` file.

For Windows:

installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\pdsys

installation-folder-for-HiCommand-Suite-Common-Component\database\work\def_pdsys

For Solaris:

/opt/HiCommand/Base/HDB/conf/pdsys

/opt/HiCommand/Base/database/work/def_pdsys

6. Edit the `pdsys` file and `def_pdsys` file.

Change the value for the `pd_hostname` parameter to the loopback address `127.0.0.1`. If the `pd_hostname` parameter does not exist, add the `pd_hostname` parameter, specifying the loopback address.

Note: For a cluster configuration, edit the `pdsys` file and `def_pdsys` file on both the executing node and standby node. In such a case, for the `pd_hostname` parameter, specify the host name for the executing node.

The following describes the storage destinations for the `pdsys` file and `def_pdsys` file:

For Windows:

installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\pdsys

installation-folder-for-HiCommand-Suite-Common-Component\database\work\def_pdsys

For Solaris:

/opt/HiCommand/Base/HDB/conf/pdsys

/opt/HiCommand/Base/database/work/def_pdsys

7. Edit the `HiRDB.ini` file.

Change the value for the `PDHOST` parameter to the loopback address `127.0.0.1`.

Note: Specify a virtual host name for a cluster configuration.

The following describes the storage destination for the `HiRDB.ini` file:

For Windows:

installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\emb\HiRDB.ini

For Solaris:

/opt/HiCommand/Base/HDB/conf/emb/HiRDB.ini

8. Edit the `cluster.conf` file (applicable only for a cluster configuration).

From among the virtual host name, host name for the executing node, and host name for the standby node, change the corresponding host name to the host name after the change.

The following describes the storage destination for the `cluster.conf` file:

For Windows:

installation-folder-for-HiCommand-Suite-Common-Component\conf\cluster.conf

For Solaris:

/opt/HiCommand/Base/conf/cluster.conf

9. Change the host name for the management server, and then restart the machine. If the host name for the management server has already been changed, just restart the machine.

10. Make sure that the HiCommand Suite Common Component service is running.

For Windows:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdssrv  
/status
```

For Solaris or Linux:

```
opt/HiCommand/Base/bin/hcmdssrv -status
```

11. Execute the `hcmdschgurl` command to change the host name in the URL for starting Web Client. For details on how to use the `hcmdschgurl` command, see section 5.5.2.

5.7 Security Settings for User Accounts

To prevent users' passwords from being guessed by a third party, HiCommand Device Manager allows password conditions (the minimum number of characters and the combination of characters that can be used) to be specified. You can also have user accounts locked automatically if the wrong password is repeatedly entered for a specific user ID.

Caution: When installing version 5.1 or later of HiCommand Suite Common Component, the user account log function and password complexity check function will be usable. These functions are enabled for users of all HiCommand Suite products, so the following problems might occur in operations of HiCommand Suite products that are version 5.0 or earlier:

- A user is unable to log in even with a correct user ID and password.
The user account might be locked. Take appropriate action such as unlocking the relevant account or registering a new user account.
- A password is unchangeable, or a user account is not addable.
The specified password might not follow the password-entry rules. Specify an appropriate password, following the output message.

The password conditions and settings related to account locking are implemented from the `security.conf` file.

In a Windows system, the `security.conf` file is stored in the following folder:

```
installation-folder-for-HiCommand-Suite-Common-Component\conf\sec
```

In a Solaris or Linux system, the `security.conf` file is stored in the following directory:

```
/opt/HiCommand/Base/conf/sec
```

The password conditions that you set in the `security.conf` file are applied when a user account is created or when a password is changed, and are not applied to passwords of existing user accounts. As a result, even if an existing password does not satisfy the password conditions, a user can use the password to log in to the system.

When you change a setting in the `security.conf` file, the change takes effect immediately.

The items you can set in the `security.conf` file are described below.

5.7.1 `password.min.length`

Specifies the minimum number of characters that can be set as a password. Specify a value in the range from 1 to 256.

Default: 4

5.7.2 `password.min.uppercase`

Specifies the minimum number of uppercase letters the password must contain. Specify a value in the range from 0 to 256. If you specify 0, no restriction applies.

Default: 0 (no restriction)

5.7.3 `password.min.lowercase`

Specifies the minimum number of lowercase letters the password must contain. Specify a value in the range from 0 to 256. If you specify 0, no restriction applies.

Default: 0 (no restriction)

5.7.4 `password.min.numeric`

Specifies the minimum number of numeric characters the password must contain. Specify a value in the range from 0 to 256. If you specify 0, no restriction applies.

Default: 0 (no restriction)

5.7.5 `password.min.symbol`

Specifies the minimum number of symbols the password must contain. Specify a value in the range from 0 to 256. If you specify 0, no restriction applies.

Default: 0 (no restriction)

5.7.6 `password.check.userID`

Specifies whether the password can be the same as the user ID. Specify `true` or `false`. When `true` is specified, passwords cannot be the same as the corresponding user ID. When `false` is specified, passwords can be the same as the corresponding user ID.

Default: `false` (passwords can be the same as user IDs)

5.7.7 `account.lock.num`

Specifies the number of unsuccessful logon attempts to allow before a user account is automatically locked. If a user makes the specified number of unsuccessful logon attempts, his or her user account will be locked. However, the `System` account cannot be locked. Specify a value in the range from 0 to 10. If you specify 0, any number of unsuccessful logon attempts is allowed.

Unsuccessful attempts to log on to other products in the HiCommand Suite that use the Single Sign-On feature count towards the number of unsuccessful logon attempts. For example, if the number of unsuccessful attempts is set to 3, and a user fails to log on to Device Manager once, fails to log on to Provisioning Manager once, and then fails to log on to Global Link Availability Manager once, his or her user account will be automatically locked.

Changing the number of unsuccessful logon attempts does not affect users who have already registered a number of unsuccessful attempts or whose user account is locked. For example, if you change the number of unsuccessful logon attempts from 5 to 2, the user account of a user who has already made three unsuccessful logon attempts will remain active. If the user then logs on successfully, or fails to log on for the fifth time, the number of unsuccessful logon attempts is reset to zero, and the setting of 2 applies from that point onward.

If a user is currently logged on and you attempt to log on using his or her account, but you fail the specified number of times, his or her user account will be locked. However, the user can continue to perform operations while still logged on.

You can unlock user accounts from a management client. You must have the User Management permission to unlock a user account. For details about unlocking user accounts, see the *HiCommand Device Manager Web Client User's Guide*.

Default: 0 (user accounts will not be locked)

5.8 Warning Banner Settings

In HiCommand Suite Common Component version 5.1 or later, an optional message (warning banner) can be displayed as a security risk measure at login. Issuing a warning beforehand to third parties that might attempt invalid access can help reduce the risk of problems such as data loss or information leakage.

The message displayable on the Login panel must be no more than 1,000 characters. If a message with the same content is registered in a different language for each locale, the message can be automatically switched to match the locale of the Web browser.

When setting up a message, you must log on as a user who has the Administrator permissions in Windows, or as the root user in Solaris or Linux.

5.8.1 Editing the Message

You edit the message in HTML format. No more than 1,000 characters can be used. In addition to the usual characters, you can use HTML tags to change font attributes or place line breaks in desired locations. (The tag characters are also counted in the number of characters.) Usable characters are from the Unicode UTF-8 encoding.

The following show an example of message editing, and the results (the warning banner) after the message has been registered.

Example of Editing a Message:

Table 5.4 Example of Editing a Message

```
<center><b>Warning Notice!</b></center>
This is a {Company Name Here} computer system, which may be accessed and used only for
authorized {Company Name Here} business by authorized personnel. Unauthorized access or use
of this computer system may subject violators to criminal, civil, and/or administrative
action.<br>All information on this computer system may be intercepted, recorded, read,
copied, and disclosed by and to authorized personnel for official purposes, including
criminal investigations. Such information includes sensitive data encrypted to comply with
confidentiality and privacy requirements. Access or use of this computer system by any
person, whether authorized or unauthorized, constitutes consent to these terms. There is no
right of privacy in this system.
```

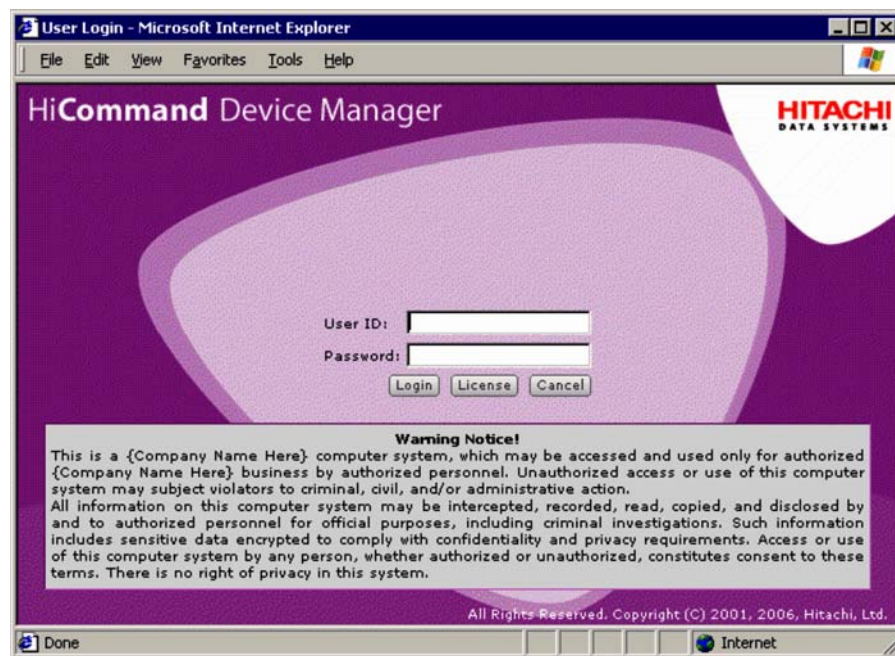


Figure 5.2 Displayed Results After Registering the Message

Caution: When the message is registered, the HTML syntax is neither checked nor corrected. Edit the message correctly in accordance with HTML syntax rules because the edited message will be registered as is. If there is an error in the HTML syntax in the message, the message might not be displayed correctly in the Login panel.

Caution: There are no restrictions on the characters usable in the message, other than that the character encoding must be Unicode (UTF-8). To display a character used in HTML syntax (e.g., <, >, ", ', &), use the HTML escape sequence. For example, to display an ampersand (&) in the Login panel, write `&` in the HTML file.

Caution: To use line breaks to display the message in a desired location, use the HTML tag `<BR>`. Even if there are linefeed characters in the message, they will be ignored when the message is registered.

Note: Sample messages in English (`bannermsg.txt`) and Japanese (`bannermsg_ja.txt`) are provided in the following locations:

- In Windows:

installation-folder-for-HiCommand-Suite-Common-Component\sample\resource

- In Solaris or Linux:

/opt/HiCommand/Base/sample/resource

These sample files are overwritten at installation so, if you wish to use a sample file, copy it and then edit it.

5.8.2 Registering the Message

You use the `hcmdsbanner` command to register an edited message.

To register a message:

1. Execute a following command:

- In Windows:

installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbanner
/add /file *file-name* [/locale *locale-name*]

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbanner /add /file  
C:\W_Banner\wbfile1 /locale en
```

- In Solaris or Linux:

```
# /opt/HiCommand/Base/bin/hcmdsbanner -add -file file-name [-  
locale locale-name]
```

file-name: Using an absolute path, specify the file that stores the message. In Solaris or Linux, do not specify a path that includes a space.

locale-name: Specify the locale of the language used for the message (e.g., `en` for English, or `ja` for Japanese). If omitted, the default locale will be specified.

Return values

0: Normal termination

253: The number of characters in the message exceeds 1,000 characters.

255: Failure

Caution: If a message for the specified locale is already registered, it will be updated by being overwritten.

Note: The execution results of the `hcmdsbanner` command are output to the file `hcmdsbannern.log`.

2. Referring to section 5.2, restart HiCommand Suite Common Component.
The message registration will go into effect.

5.8.3 Deleting the Message

You use the `hcmdsbanner` command to delete a registered message.

To delete a message:

1. Execute a following command:

- In Windows:

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbanner  
/delete [/locale locale-name]
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbanner /delete /locale  
en
```

- In Solaris or Linux:

```
# /opt/HiCommand/Base/bin/hcmdsbanner -delete [-locale locale-  
name]
```

locale-name: Specify the locale of the message to be deleted (e.g., `en` for English, or `ja` for Japanese). If omitted, the default locale will be specified.

Return values

0: Normal termination

254: A message of the specified locale has not been registered.

255: Failure

Note: The execution results of the `hcmdsbanner` command are output to the file `hcmdsbannern.log`.

2. Referring to section 5.2, restart HiCommand Suite Common Component.
The message deletion will go into effect.

Chapter 6 Setup for Managing Copy Pairs

This chapter discusses the following setup requirements:

- Server Requirements for Managing Copy Pairs (see section 6.1)
- Host requirements (see section 6.2)
- Subsystem requirements (see section 6.3)
- CCI and Protection Manager requirements (see section 6.4)

6.1 Server Requirements for Managing Copy Pairs

- You can use Device Manager to control copy pairs in one of two ways:
 - Local management, with each host managing the copy pair(s) for the LUs recognized by that host.
 - Central management, with a single host managing all of the copy pair(s) for the LUs recognized by multiple hosts. This requires Device Manager version 3.0 or higher. The `server.agent.rm.centralizePairConfiguration` property file for Device Manager Agent must be set to enable.
- The subsystems that are candidates for P-VOL or S-VOL must be managed by a single Device Manager Server.
- The Device Manager Server must recognize the host that has the Device Manager Agent installed.

6.2 Host Requirements for Managing Copy Pairs

Device Manager Agent must be installed on the host. Table 6.1 lists the Web Client operations and required versions of Device Manager Agent.

Table 6.1 Copy Pair Operations and Required Versions of Device Manager Agent

Function	Pair Operation	Required Version
ShadowImage and TrueCopy	Displays the status.	2.3 or later
ShadowImage	Display the status (maximum 1:3).	5.5 or later
ShadowImage and TrueCopy	Changes the status.	2.4 or later
ShadowImage	Change the status (maximum 1:3).	5.5 or later
QuickShadow	Changes the status.	3.0 or later
QuickShadow	Change the status (maximum 1:15).	5.5 or later
Universal Replicator	Displays the status.	4.0 or later

Universal Replicator	Display the 3DR status.	5.5 or later
COW Snapshot	Change the status.#	4.1 or later

The status can only be changed on the TagmaStore AMS/WMS series. On TagmaStore USP, the status can only be displayed.

- Device Manager Agent must be one of the following versions:
 - 2.3 or later to display the status of a copy pair.
 - 2.4 or later to change the status of a ShadowImage or TrueCopy copy pair.
 - 3.0 or later to change the status of a QuickShadow copy pair.
 - 4.0 or later to display the copy status of a Universal Replicator pair.
- RAID Manager must be installed on the host. If copy pairs for the Lightning/Thunder series and StorageWorks XP Disk Array are managed on one host, both CCI and RAID Manager XP must be installed. For details on how to install CCI and RAID Manager XP, see the manuals for CCI and RAID Manager XP.
- If you are using central management, you do not need to install CCI and Device Manager Agent on all of the hosts. Device Manager need only be installed on a host that centrally manages copy pairs, because the other hosts can recognize the copy pairs in that host. In order for the LUs to be recognized by the host, that host must have LUN security enabled.
- The host must be able to recognize the subsystem that will be used as a command device.
- The host must be able to recognize the subsystems that are candidates for P-VOL or S-VOL.
- To display the copy pair status, the host must recognize the P-VOL that makes up the copy pair.
- To change the copy pair status, the host must recognize the P-VOL and S-VOL that make up the copy pair or that are a candidate for a copy pair. In the central management method, the host that centrally manages copy pairs does not need to recognize the P-VOL and S-VOL that make up a copy pair or that are a candidate for a copy pair.
- CCI must have fewer than 32 running instances.
- You cannot use ports 53232 through 53263.
- The Device Manager agent must be restarted as part of the setup.

Caution: You can use the 9900 Remote Console, 9900V Storage Navigator, SVP, or CCI library to create or manage a copy pair without using CCI. However, you cannot change the status of or delete such copy pairs from Device Manager, because there is no configuration definition file for operating such a copy pair using CCI. If you have an existing copy pair that was not created using CCI, first release the copy pair (using the same tool that created it), and then use Device Manager to re-create the volume pairs.

6.3 Subsystem Requirements for Managing Copy Pairs

- Command Control Interface (CCI) must be installed and enabled, in the following versions:
 - To use TrueCopy or ShadowImage: 01-10-03, 01-11-03, or 01-12-03/04
 - To use QuickShadow: 01-12-03/04
- Command Device Security must be installed. This requires Resource Manager.
- CCI must have fewer than 32 running instances.
- You cannot use ports 53232 through 53263.
- The P-VOL or S-VOL pairs created by ShadowImage must be recognizable. The S-VOL pairs must be recognizable if cascaded.
- The P-VOL or S-VOL pairs created by TrueCopy must be recognizable.
- After the subsystem has been configured as required, the subsystem must be refreshed.
- The subsystem serial numbers managed by Device Manager must all be unique. In the case of TrueCopy, remote subsystems that are not managed by Device Manager must also have unique serial numbers.
- For 9200, the default serial number of the storage subsystem must not have been changed.

Caution: You can use the 9900 Remote Console, the 9900V Storage Navigator, the SVP or CCI library to create or manage a copy pair without using CCI. However, you cannot change the status of or delete such copy pairs from Device Manager, because there is not a configuration definition file for operating such a copy pair with CCI. If you have an existing copy pair that was not created using CCI, first release the copy pair (using the same tool that created it) then use Device Manager to re-create the volume pairs.

Table 6.2 Subsystem Requirements

Subsystem	Function	Requirements
TagmaStore Universal Storage Platform, Lightning 9900V, Lightning 9900	TrueCopy	TrueCopy or TrueCopy Asynchronous must be enabled. There must be a fibre-channel connection between the two ports used for an MCU-RCU path. The MCU port for a MCU-RCU path must be an Initiator port, and the RCU port must be an RCU Target port. The RCU and the MCU-RCU path must be registered in the MCU. Note: To change the port configuration, use the TagmaStore USP or 9900V Storage Navigator or the 9900 Remote Console. Refresh the Device Manager server after you configure the ports. The subsystem cache or non-volatile storage must be sufficient. See <i>Hitachi TagmaStore USP and NSC Universal Storage Platform TrueCopy User and Reference Guide</i>, <i>Hitachi Lightning 9900 V Series TrueCopy User and Reference Guide</i> or <i>Hitachi Lightning 9900 TrueCopy User and Reference Guide</i> for more information about TrueCopy, including instructions for changing the port configuration and a description of the required cache. Note: You can use the TagmaStore USP or 9900V Storage Navigator or the 9900 Remote Console to confirm the amount of cache. Contact your

		Hitachi Data Systems representative if you need to add cache.
	ShadowImage	ShadowImage must be enabled. For TagmaStore AMS/WMS series, a DM-LU must be set up. For more information about ShadowImage please see the following <i>Hitachi TagmaStore USP and NSC ShadowImage User's Guide</i> , <i>Hitachi Lightning 9900V Series ShadowImage User's Guide</i> or <i>Hitachi Lightning 9900 ShadowImage User's Guide</i> .
TagmaStore AMS/WMS Series, Thunder 9500V	TrueCopy	TrueCopy Basic or TrueCopy Extended Distance must be enabled. There must be a fibre-channel connection between the two ports used for a path. The TrueCopy path must be configured. The data share mode must be ON. The system start attribute must be dual active mode. The SCSI ID/Port ID inheritance mode must be set to Unused. For TagmaStore AMS/WMS Series, a DM-LU must be set up. For more information about TrueCopy please see <i>Hitachi Thunder 9500 V Series TrueCopy User's Guide</i> .
	ShadowImage	ShadowImage must be enabled. If you have installed TrueCopy Basic, you can also use ShadowImage. The data share mode must be ON. The system start attribute must be dual active mode. The SCSI ID/Port ID inheritance mode must be set to Unused. For TagmaStore AMS/WMS Series, a DM-LU must be set up. For more information about ShadowImage please see <i>Hitachi Thunder 9500 V Series ShadowImage User's Guide</i> .
TagmaStore AMS/WMS Series, Thunder 9500V	Copy on Write Snapshot, QuickShadow	QuickShadow must be enabled. Restart the subsystem after installation. For QuickShadow, unlike ShadowImage and TrueCopy, you can only specify a V-VOL, which is a special LU prepared in advance, as an S-VOL. To configure QuickShadow or Copy on Write Snapshot: - Create a QuickShadow pool. - In the QuickShadow Pool, define the V-VOL. Note: For the TagmaStore AMS/WMS series, the product name is COW Snapshot. For the TagmaStore AMS/WMS series, a DM-LU must be set up.
Thunder 9200	TrueCopy	TrueCopy Synchronous must be enabled. There must be a fibre-channel connection between the two ports used for a path. The Remote Copy path must be configured. The data share mode must be ON. The system start attribute must be dual active mode. The SCSI ID/Port ID inheritance mode must be set to Unused. Specify the INQUIRY data extended mode in the host mode 2 to all the ports. For more information on TrueCopy please see <i>Hitachi Thunder 9200 TrueCopy User's Guide</i> .
	ShadowImage	ShadowImage Lite must be enabled. The stripe size must be configured as 64 KB. The data share mode must be ON.

		The system start attribute must be dual active mode. The SCSI ID/Port ID inheritance mode must be set to Unused. Specify the INQUIRY data extended mode in host mode 2 to all ports. For more information on ShadowImage please see <i>Hitachi Thunder 9200 ShadowImage User's Guide</i>.
--	--	---

6.4 Creating Configuration Definition Files

You can use Device Manager to create a configuration definition file, which is then used by CCI to create copy pairs. This requires Device Manager Agent installed on each host at version 3.1 or higher.

Device Manager has the following features when interacting with CCI:

- You cannot use Device Manager to create a copy pair. You must use CCI.
- You cannot use Device Manager to delete an invalid configuration file, even if you created that file with Device Manager. You must use CCI. This is important, because an invalid configuration file can adversely affect system performance.

To create a configuration definition file:

1. If a copy pair is already managed by CCI, the copy pair can be managed by Device Manager after Device Manager is installed. Similarly, if the copy pair is managed by Protection Manager, the copy pair can be managed by Device Manager after Device Manager is installed.

Note: When Device Manager is installed, the Device Manager Agent property must be configured if the installation drive of CCI in Windows is different from the installation drive of Device Manager Agent.

2. When you directly use CCI or exclude the copy pair managed by Protection Manager from Device Manager operations, the following actions are required:
3. Check the HORCM instance number of CCI managing the copy pair.
4. In the following property in the Device Manager Agent property file, enter the HORCM instance that you want to exclude from Device Manager operations. Separate HORCM instances by commas if you want to enter multiple HORCM instances:
 - Property file name: server.properties.
 - Property name: server.agent.rm.exclusion.instance.

Example:

server.agent.rm.exclusion.instance=0, 1, 2

- Restart the Device Manager Agent service (daemon).

6.4.1 Using Device Manager Web Client to Create a Configuration Definition File for CCI

Device Manager Web Client allows you to create a configuration definition file. This configuration definition file is used when CCI is used to create copy pairs.

Note: This function is provided for system administrators who use CCI to manage copy pairs.

Caution: You cannot use the configuration definition file created by this function to create a copy pair by using Device Manager.

- You cannot use Device Manager to delete an invalid configuration file if the file was created by this function. To delete or edit such a configuration file, execute the appropriate CCI command from a host.
- An invalid configuration file or a configuration file that is not used for operating copy pairs may affect system performance: for example, when discovering a subsystem or refreshing information. To delete such a configuration file, execute the appropriate CCI command from a host.
- Requirements for the function for creating the configuration definition file:
 - The storage subsystem and host satisfy the requirements described in sections 6.1, 6.2, and 6.3.
 - The version of Device Manager agent installed on the host is 3.1 or later.
- Using the function for creating the configuration definition file:

To create a configuration definition file:

1. Stop the HBase Storage Mgmt Common Service. (For instructions on how to do that, see section 5.2.2.)
2. Set the value of the `client.outputhorcmfunction.enabled` property in the `client.properties` file to `true`. For details about the `client.outputhorcmfunction.enabled` property, see section 8.7.3.)
3. Start the HBase Storage Mgmt Common Service. (For instructions on how to start the HiCommand Single Sign On Service, see section 5.2.2.)
4. Start the operation for creating a copy pair. (For instructions on how to create a copy pair, see the HiCommand Device Manager Web Client User's Guide.

Caution: When managing pairs by each host, Device Manager Agent version 3.1 or later must be installed on the host to be used. When managing pairs by central management, Device Manager Agent version 3.1 or later must be installed on the host that centrally manages the pairs.

5. Perform the operation in the same manner as when creating a copy pair to display the **Step: Summary Of Changes** dialog box.

Note: In the **Step: Define Pair(s)** dialog box, you do not need to specify the fence level and copy pace. Even if you specify these items, they are not applied in the configuration definition file.

6. In the **Step: Summary Of Changes** dialog box, click **Cancel (Output HORCM)** to stop creating a copy pair, and then start creating the configuration definition file.
7. When creation of the configuration definition file finishes, a dialog box appears notifying you of the completion. Check the display, and then click the **Close** button.

In the View Pair Information dialog box, you can view the HORCM instance number, pair group name, and pair name of the created configuration definition file.

Caution: For a Shadow Image copy pair and a QuickShadow or COW Snapshot copy pair, Device Manager sets 0 as the MU number in the configuration definition file. (Note that, for TrueCopy, the MU number is not set because this number is not necessary.) When you use a configuration definition file created by Device Manager to create a copy pair, make sure that you change this value to an appropriate value.

Chapter 7 HiCommand Device Manager Server Security

This chapter provides an overview of Device Manager security and explains procedures for setting up security.

- Overview of HiCommand Device Manager Security (see section 7.1)
- Using HiKeytool to Set Server Security (see section 7.2)
- Configuring the HBase Storage Management Web Service for SSL (see section 7.3)
- Security Settings for CIM/WBEM Functionality (see section 7.4)
- Authenticating File Operations Using a Java Tool (see section 7.5)

7.1 Overview of HiCommand Device Manager Security

This section discusses the following server security procedures:

Note: Screen shots in this section are from Windows, unless otherwise indicated.

7.1.1 About Server and HBase Storage Mgmt Web Service Security

HiCommand Device Manager uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to encrypt network transmissions between the Device Manager client and the Device Manager Server or the HBase Storage Mgmt Web Service. SSL and TLS use cryptography, digital signature technology and digital certificates to provide user authentication, data integrity, and privacy. This document includes instructions for configuring Device Manager to securely communicate over the Internet or an Intranet using SSL and TLS.

WARNING: If you are using Internet Explorer, set your options so that encrypted pages are not saved to disk.

Important: If you enable security on Device Manager, you must make sure that the key pair and associated server certificate do not expire. If either the key pair or the server certificate expires, users will be unable to connect to the Device Manager Server or HBase Storage Mgmt Web Service with the Device Manager Web Client. See section 7.2.1 for instructions.

Note: If you use SSL-encrypted communication, you must enter `https://` in the browser when sending a request.

This chapter includes the following terms:

- **<host name>** is used to indicate the name of the host that is running the Device Manager Server or HBase Storage Mgmt Web Service, unless otherwise indicated.
- **<Java Web Start>** is used to indicate the default Java Web Start installation directory on a client machine. If a client's Java Web Start directory is not located in the default location, adjust commands or paths accordingly. The default directories are as follows:

For Windows:

C:\Program Files\Java Web Start

For Solaris or Linux:

\$HOME/utils/webstart/javaws

- **<server installation directory>** is used to indicate the default Device Manager Server installation directory. If your directory is not located in the default directory, adjust commands or paths accordingly. The default server installation directories are as follows:

For Windows:

C:\Program Files\HiCommand\Device Manager

For Solaris or Linux:

/opt/HiCommand/

- **Public Key Infrastructure (PKI)** is a cryptographic technology developed under the guidance of the Internet Engineering Task Force (IETF) to create a secure networking system that can have interoperative characteristics between multiple vendors.
- **Secure Sockets Layer (SSL)** is a protocol first developed by Netscape® to securely transmit data over the Internet. Two SSL-enabled peers use their Private and Public Keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.
- **Transport Layer Security (TLS)** is the successor protocol to SSL. For more information, see the RFC, The TLS Protocol (version 1.0), located on <ftp://ftp.isi.edu/in-notes/rfc2246.txt>.
- A **keypair** is two mathematically-related cryptographic keys consisting of a Private Key and its associated Public Key.
- A **keystore** is a file that contains the keypair, which is used for TLS/SSL connections and the corresponding server certificate.
- A **keypass** is a password for restoring the keypair used to encrypt TLS/SSL connections and the corresponding server certificate.
- A **truststore** is a file containing a signed and trusted server certificate.

- A **Server Certificate** (sometimes also called a **Digital Certificate**) forms an association between an identity (in this case the Device Manager Server or the HBase Storage Mgmt Web Service) and a specific keypair. A Server Certificate is used to identify the Device Manager Server or HBase Storage Mgmt Web Service to a client so that the server and client can communicate using TLS/SSL. Server Certificates come in two basic types:
 - Self-signed: (see sections 7.2.1 and 7.3.3). This is the case where you generate your own certificate, so that the subject of the certificate is the same as the issuer of the certificate. For example, when you create a keypair with HiKeytool, you will have a keypair and an associated self-signed certificate.
 - Signed and Trusted: (see sections 7.2.3 and 7.3.2). When a Certificate Signing Request (CSR) is generated and sent to a well-known and trusted Certificate Authority (CA) for signing, and is then signed and returned by the Certificate Authority, your certificate is considered signed and trusted. A well-known and trusted Certificate Authority meets the following requirements:
 1. Certificate for that Certificate Authority is located inside the Device Manager Server truststore,
 2. Certificate for that Certificate Authority is located in the database of trusted Certificate Authorities within browsers supported by Device Manager, and
 3. Certificate for that Certificate Authority is located within the truststore distributed with Java Web Start.

Note: The default Device Manager Server truststore is located at **<installation directory>/jre/lib/security/cacerts**. You can modify the default location using the **server.https.security.truststore** property in the server.properties file (see section 8.8.8). The default truststore for Java Web Start is located at **<Java Web Start installation directory>/cacerts**.

7.2 Using HiKeytool to Set Server Security

7.2.1 Creating a Keypair

Throughout this section, use the default values presented unless you are either very familiar with the area of cryptography and Java(TM) security or are otherwise instructed.

Note: If you make a mistake during this process and need to start over, exit by typing Ctrl+C and restart HiKeytool.

1. Open a command prompt or terminal window, navigate to the *<HiCommand server>* directory and launch HiKeytool, as follows:
 - For Windows, type **HiKeytool.bat**, and then press **Enter**.
 - For Solaris or Linux, log on as the root user. Type **HiKeytool.sh** and press **Enter**.
2. The HiKeytool main panel (see Figure 7.1) appears Enter 1.
3. The server main panel appears (see Figure 7.2). Enter 1 (**Make Keypair/Self-Signed Certificate**). The Creating a Keypair panel appears (see Figure 7.3).
4. Enter the server name [default=sasol03]. Use the default value unless your machine is visible to the LAN or WAN under a different name, in which case you should use the name by which the Device Manager Server is visible. Any SSL-encrypted communications with the server **MUST** use this server name, or you will receive an authentication error.
5. Enter the organizational unit [default= *Device Manager Administration*]. The default value is recommended, but you can use anything meaningful, for example, Marketing.
6. Enter your organization name. Ordinarily you would use the default value or your host name, but you can use another name, such as the name of your company.
7. Enter your city or locality. There is no default value for this field.
8. Enter your state or province. Make sure to spell it out instead of using an abbreviation. There is no default provided.
9. Enter your two-character country code [default=US].
10. Enter your key alias. [default=sasol03]. This should be the local host name of the Device Manager Server. Make sure to use the same value that you previously used for the server name.
11. Enter your key password (6 characters minimum) [default=passphrase]. This is the value used to access the keypair entry by the Device Manager Server and the default value is taken from the server.https.keystore.keypass property (see section 8.8.6).
12. For security reasons, you will want to change the default value of the key password.

Important: You should do so by using the process described in section 7.2.7, and you should not simply change it directly from the properties file.
13. Enter the key algorithm [default=RSA]. Currently, only RSA® is supported.

14. Enter the key size (minimum is 512; maximum is 2048, default=2048]. Assuming the RSA® key algorithm is used, any key size from 512 to 2048 is valid, so long as it is a multiple of 64. Larger key sizes are recommended because that will provide greater data security against brute force and factoring attacks.
15. Enter the signature algorithm [default=MD5withRSA]. Currently, only MD5withRSA is supported.
16. Enter the number of days valid [default=365]. This is the period during which the Device Manager Server keypair will be valid:
 - If you have your server certificate signed by a well-known and trusted Certificate Authority, the number of days valid specified by that authority will override the value you place in this field. Make sure to check the web site of your vendor for specific requirements and calendar the need to renew your certificate, because if the key pair and associated server certificate expire, users will be unable to establish a secure connection with the Device Manager Server via SSL/TLS.
 - If you elect not to have your server certificate signed, the value that you place in this field will determine the period during which the keypair and associated server certificate will be valid. The default is 365 days.
17. Enter the keystore password (6 characters minimum) [default=passphrase]. This is the value used to protect and verify the integrity of the keystore, and the default value is taken from the `server.https.keystore.passphrase` property (see section 8.8.5).

Important: If you want to change the default value of the keystore password, you should use the process described in section 7.2.7. Do not change it directly from the properties file.
18. Once you have completed these steps, Device Manager will generate the Device Manager Server keypair and associated certificate. The keypair is placed inside the keystore for the Device Manager Server.

Note: If you create a keypair with a size of 2048 you might have to wait up to a minute for the keypair to generate.

You will need to restart the Device Manager server for the changes to be implemented.

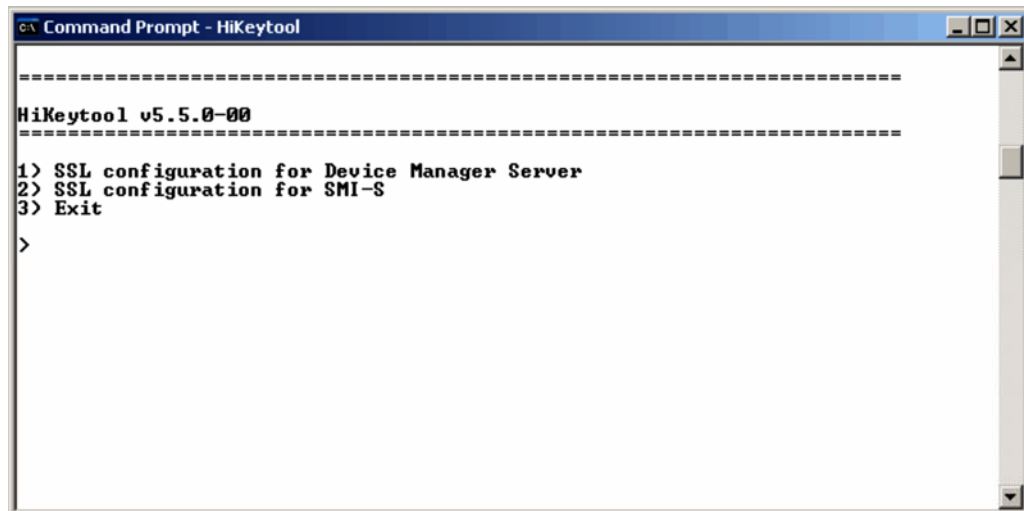


Figure 7.1 HiKeytool Main Panel

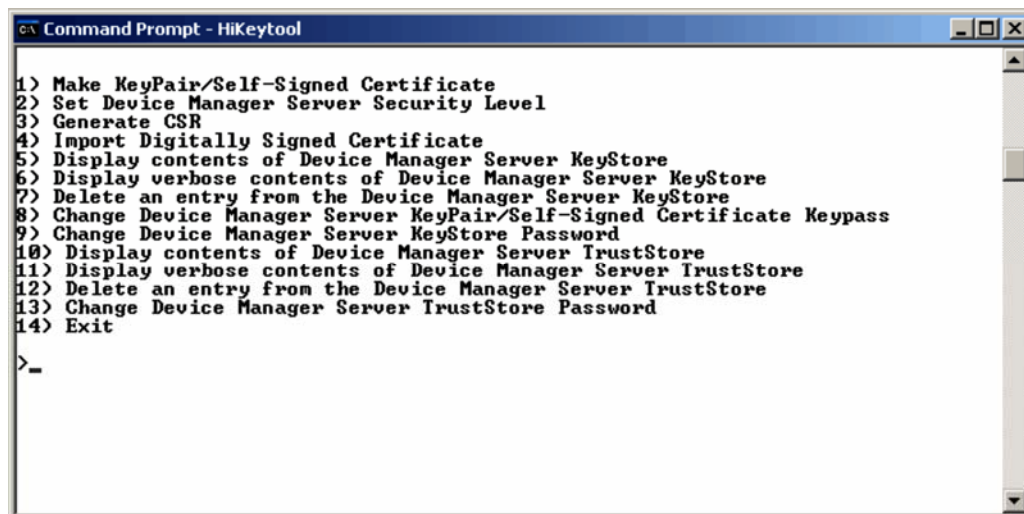
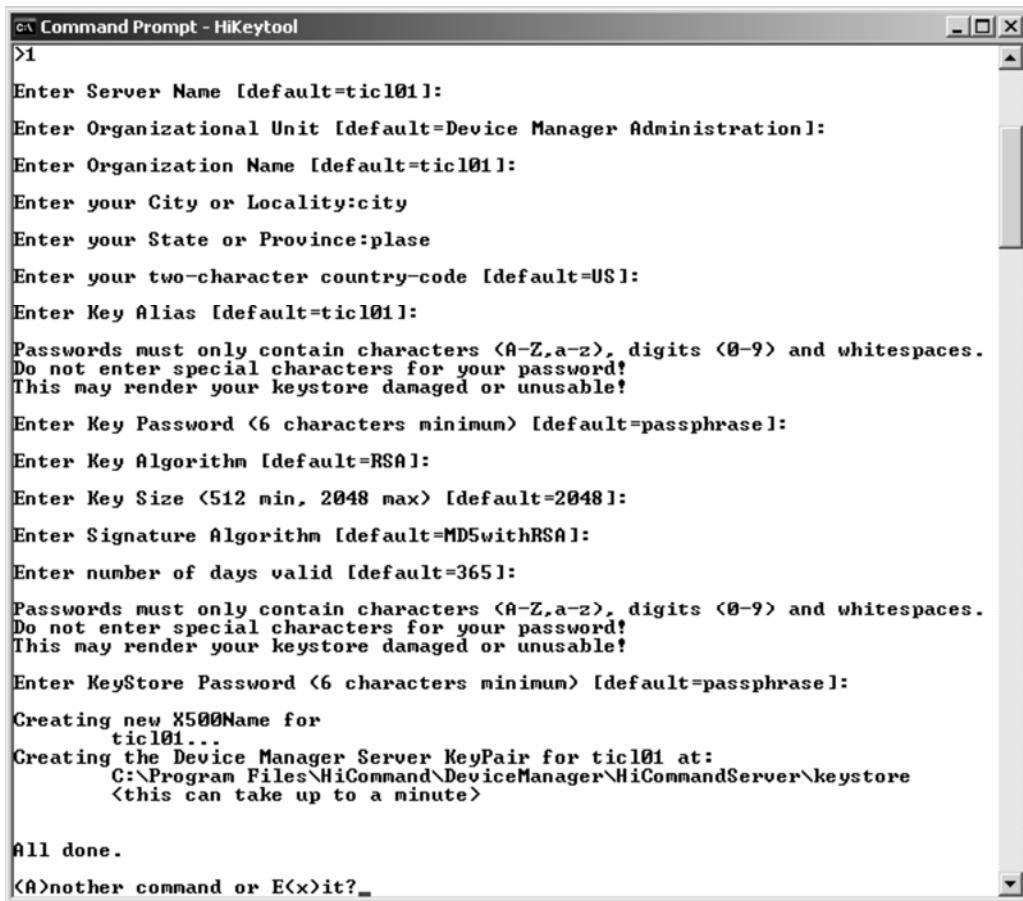


Figure 7.2 Server Main Panel



```
CA Command Prompt - HiKeytool
>1
Enter Server Name [default=ticl01]:
Enter Organizational Unit [default=Device Manager Administration]:
Enter Organization Name [default=ticl01]:
Enter your City or Locality:city
Enter your State or Province:plase
Enter your two-character country-code [default=US]:
Enter Key Alias [default=ticl01]:
Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!
Enter Key Password (6 characters minimum) [default=passphrase]:
Enter Key Algorithm [default=RSA]:
Enter Key Size (512 min, 2048 max) [default=2048]:
Enter Signature Algorithm [default=MD5withRSA]:
Enter number of days valid [default=365]:
Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!
Enter KeyStore Password (6 characters minimum) [default=passphrase]:
Creating new X509Name for
    ticl01...
Creating the Device Manager Server KeyPair for ticl01 at:
    C:\Program Files\HiCommand\DeviceManager\HiCommandServer\keystore
    <this can take up to a minute>

All done.
<A>nother command or E<x>it?_
```

Figure 7.3 Creating a Keypair

7.2.2 Enabling TLS/SSL Server Security

Important: TLS and SSL require Internet Explorer 5.5 or Netscape® 6.0 or higher.

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 2 (**Set Device Manager Server Security Level**).
3. HiKeytool will echo the current security level, display the three available levels of security, and prompt the user for an entry (see Figure 7.4), as follows:
 - 0 Unsecure, no security.
 - 1 Basic authentication, which requires a valid username and password.

Note: This is the default. Information will be base64 encoded, but it can be easily unencoded and read by anyone listening to the communications being sent on a network.

- 2 Encrypted using TLS/SSL, which is discussed in this section.
4. To enable TLS/SSL (Secure Sockets), type 2 and press **Enter**. The display will confirm that you have selected TLS/SSL (see Figure 7.5).
 5. You will need to restart the Device Manager Server for these changes to take effect.

Note: If you only want to use a self-signed certificate, skip the next sections and go directly to section 7.3.1 and continue from that point.

```
Command Prompt - .\hikeytool.bat

1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

>2

Current Device Manager Server Security Level = User Logon <Basic Authentication>

Options:
0) Unsecure <None>
1) User Logon <Basic Authentication>
2) TLS/SSL <Secure Sockets>
Enter selection: [default=1]:_
```

Figure 7.4 Default Device Manager Server Security Level

```
Command Prompt - .\hikeytool.bat

5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

>2

Current Device Manager Server Security Level = User Logon <Basic Authentication>

Options:
0) Unsecure <None>
1) User Logon <Basic Authentication>
2) TLS/SSL <Secure Sockets>
Enter selection: [default=1]:2

Device Manager Server Security level set to: TLS/SSL Secure Socket
You must restart the Device Manager Server for this change to take effect.

<A>nother command or E<x>it?
```

Figure 7.5 Selecting and Confirming Server Security Level Changes

7.2.3 Creating and Importing a Digitally-Signed Certificate

This section contains instructions for obtaining a digitally-signed certificate from a well known and trusted Certificate Authority. See section 7.1 for a discussion of the merits of using digitally-signed certificates.

7.2.3.1 Creating a Certificate Signing Request (CSR)

To create a Certificate Signing Request:

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 3 (Generate CSR).
3. HiKeytool will inform the user where the Certificate Signing Request has been stored on disk (see Figure 7.6), which will be in a file named <host name>.csr inside the <Device Manager Server> directory. The contents of your CSR will look similar to the example in Figure 7.7.

Important: Your CSR will contain extra carriage returns and line feeds which must be included when it is sent to the Certificate Authority, or it will not be processed correctly.

4. You will then send the CSR to the Certificate Authority of your choice to be digitally signed. The application for digital signing can be done online, and the response is typically returned to you via email from the Certificate Authority.
5. If you intend to have a self-signed certificate digitally signed by a Certificate Authority, you may want to check their web site for specifics. If your Certificate Authority's requirements are sufficiently different, you may want to re-create the Device Manager Server keypair before generating a CSR. To re-create the keypair (see section 7.2.9 for instructions), and then create a new keypair as described in section 7.2.1.

Note: There must be only one entry in the Device Manager Server keystore, or you could have problems when you are running the Device Manager Server in secure mode.

```

Command Prompt - .\hikeytool.bat

=====
1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

>3

Generating CSR...
CSR has been written to disk and saved at:
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\tic101.csr
All done!

<A>nother command or E(x)it?_

```

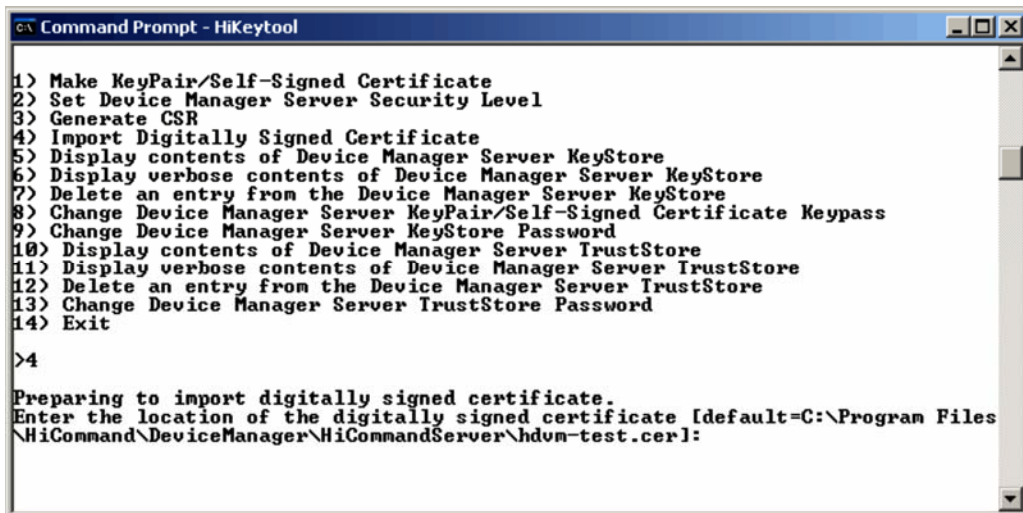
Figure 7.6 Completed CSR

```

---BEGIN NEW CERTIFICATE REQUEST-----
MIICzDCCAbQCAQAwYYxCzAJBgNVBAYTA1VITMRMwEQYDVQQIEWpDYWxpZm9ybm1hMRQwEgYDVQQQH
EwtMb3MgQW5nZWxlczEQA4GA1UEChMHAGlzaGFyZzEoMCYGA1UECzMfSG1Db21tYW5kIFNlcnZ1
ciBBZG1pbmlzdHJhdGlvb3JlYQMA4GA1UEAxMHAGlzaGFyZzCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALH9cjGweKgcjqcNEBAJyduJkvOkov5UGrEFQXsVBGgq3F30W5PD83E1WfS0+UJU
BHPE7YI5A/yc8Irtbhn+muXHC/+q1KIIZNTAunt0ta2JuhqK5fR22rJh6wCwvzmOwEZJAINPNUW
SN7w1OLsZ7dPJHAQs4KJBsrG9Gh3+KBU0gFMK080lmHPP9e8vfGfQo1YdSqOddQLyHktQxhmktQ
l3adMMsXykjS4SCFea1TuLcLRaNHg4Q9mPF+YiVmdcqCEXorhQhcMh3iL/AcOrRAQ9GBFZ1xg2Wn
nA8XawVOeWcdB0Dr9W9TWaKNSAAS5xcF0vxxkCZQ01Z+5iTdWdc0CAwEAAaAAMA0GCSqGSIb3DQEB
BAUAA4IBAQBfMbLbYOZJ2JWJohGNk1TY8HYv0DNiUlanuADS7gc0/iLX5/9amexHePxRhIthmih7
C1CoR+IvNlJxhzqVhgl9noLgbqQhTffIClGA2COvdFN8VPzeLidch94XaaJfSJ44U29iVgNDSuft
bEk124mimGbDdczRxooDms9pSiI2oCtRwFA7zUXSGO7NquKkPaExO+fM6s5cnTlNew5HE8e6jfoL
e65g9/6hcH7KacbwkRzU9R4iMrcOhW6HnlV0GDeCyhmAEW0dsHSwaBptEM3gGo+ffXhL54tXX771
tnYJU1QAjfrRqTi9eFL4N2Ooo4An8jXYooBjknolr+X+V4r
-----END NEW CERTIFICATE REQUEST-----

```

Figure 7.7 Sample Certificate Request



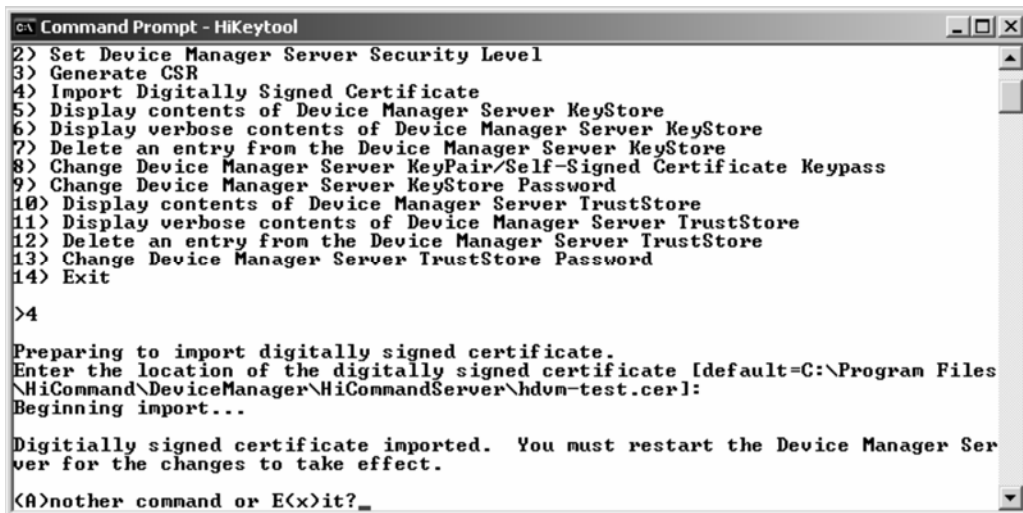
```
CA Command Prompt - HiKeytool

1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

>4

Preparing to import digitally signed certificate.
Enter the location of the digitally signed certificate [default=C:\Program Files
\HiCommand\DeviceManager\HiCommandServer\hdm-test.cer]:
```

Figure 7.9 Entering the Location of the Digitally-Signed Certificate Location (Windows)



```
CA Command Prompt - HiKeytool

2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

>4

Preparing to import digitally signed certificate.
Enter the location of the digitally signed certificate [default=C:\Program Files
\HiCommand\DeviceManager\HiCommandServer\hdm-test.cer]:
Beginning import...

Digitally signed certificate imported. You must restart the Device Manager Ser
ver for the changes to take effect.

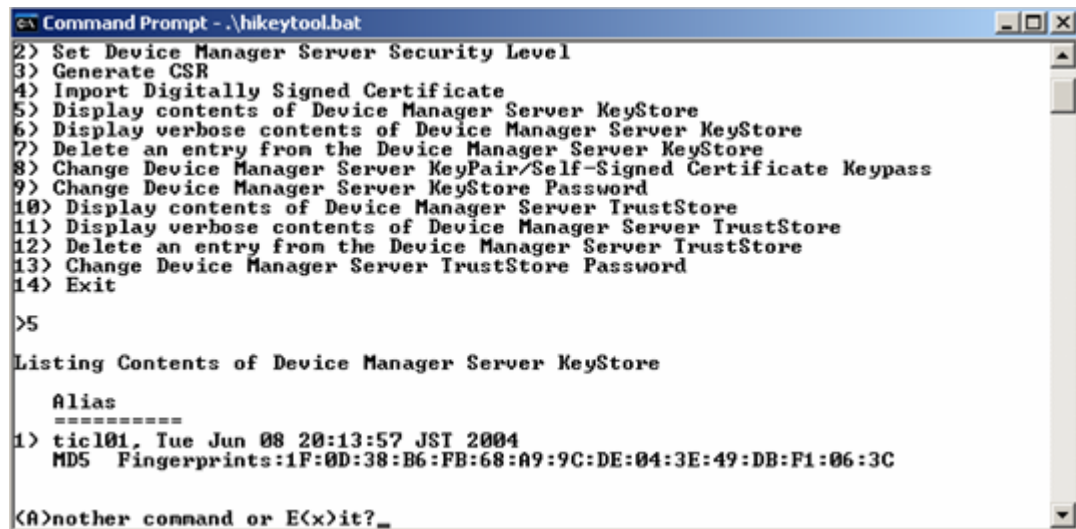
<A>nother command or E<x>it?_
```

Figure 7.10 Notification of Successful Import of Digitally-Signed Certificate

7.2.4 Displaying Contents of the HiCommand Device Manager Keystore

7.2.4.1 Regular Mode

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 5 (Display Contents of Device Manager Server Keystore).
3. HiKeytool will display information similar to that in Figure 7.11, including the alias for the keystore entry, the date the entry was created, and the MD5 Fingerprints for the entry, as follows:



```
Command Prompt - .\hikeytool.bat
2> Set Device Manager Server Security Level
3> Generate CSR
4> Import Digitally Signed Certificate
5> Display contents of Device Manager Server Keystore
6> Display verbose contents of Device Manager Server Keystore
7> Delete an entry from the Device Manager Server Keystore
8> Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9> Change Device Manager Server Keystore Password
10> Display contents of Device Manager Server TrustStore
11> Display verbose contents of Device Manager Server TrustStore
12> Delete an entry from the Device Manager Server TrustStore
13> Change Device Manager Server TrustStore Password
14> Exit
>5
Listing Contents of Device Manager Server Keystore
  Alias
  =====
1> ticl01, Tue Jun 08 20:13:57 JST 2004
   MD5 Fingerprints:1F:0D:38:B6:FB:68:A9:9C:DE:04:3E:49:DB:F1:06:3C
<A>nother command or E<x>it?_
```

Figure 7.11 Sample Contents of Device Manager Server Keystore

7.2.4.2 Verbose Mode

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 6 (Display Verbose Contents of Device Manager Server Keystore).
3. HiKeytool will display the verbose contents of the Device Manager Server keystore (see Figure 7.12 for a sample).

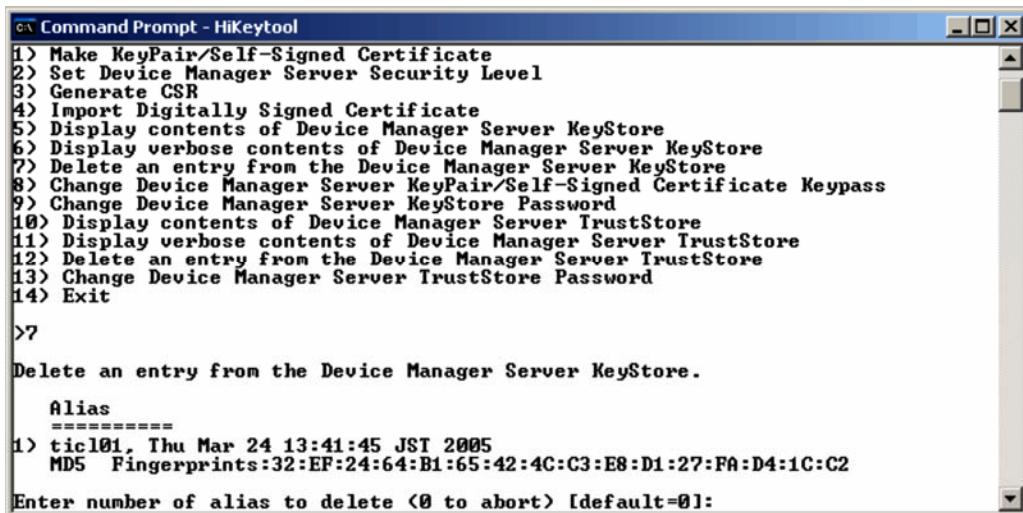


```
Command Prompt - .\hikeytool.bat
>6
Listing Contents of Device Manager Server Keystore
1)
alias: ticl01
Certificate chain length: 1
Issued by: ticl01:ticl01
Server Name: ticl01
Organizational Unit: HiCommand Device Manager Administration
Organization: ticl01
Locality: Your City
State: Some place
Country: US
Created: Tue Jun 08 20:13:57 JST 2004
Entry Type: Key Entry
Certificate Version: 1
Serial Number: 40c59f75
Valid from: Tue Jun 08 20:13:57 JST 2004
Valid to: Wed Jun 08 20:13:57 JST 2005
Certificate: VALID
MD5 Fingerprints: 1F:0D:38:B6:FB:68:A9:9C:DE:04:3E:49:DB:F1:06:3C
SHA1 Fingerprints: 78:E2:F6:29:4D:63:9A:1F:E6:5F:52:59:E3:48:CD:C7:2A:28:19:5D
<A>nother command or E<x>it?_
```

Figure 7.12 Sample Verbose Contents of Device Manager Server Keystore

7.2.5 Deleting an Entry from HiCommand Device Manager Server Keystore

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 7 (Delete an Entry from the Device Manager Server Keystore).
3. This will display information about the contents of the Device Manager Server keystore, and prompt you to enter the number of the Device Manager Server keypair to be deleted (see Figure 7.13).
4. HiKeytool will request confirmation of the delete (see Figure 7.14). Enter Y to confirm the delete.
5. HiKeytool will display the contents of the Device Manager Server keystore after the deletion.



```
Command Prompt - HiKeytool
1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

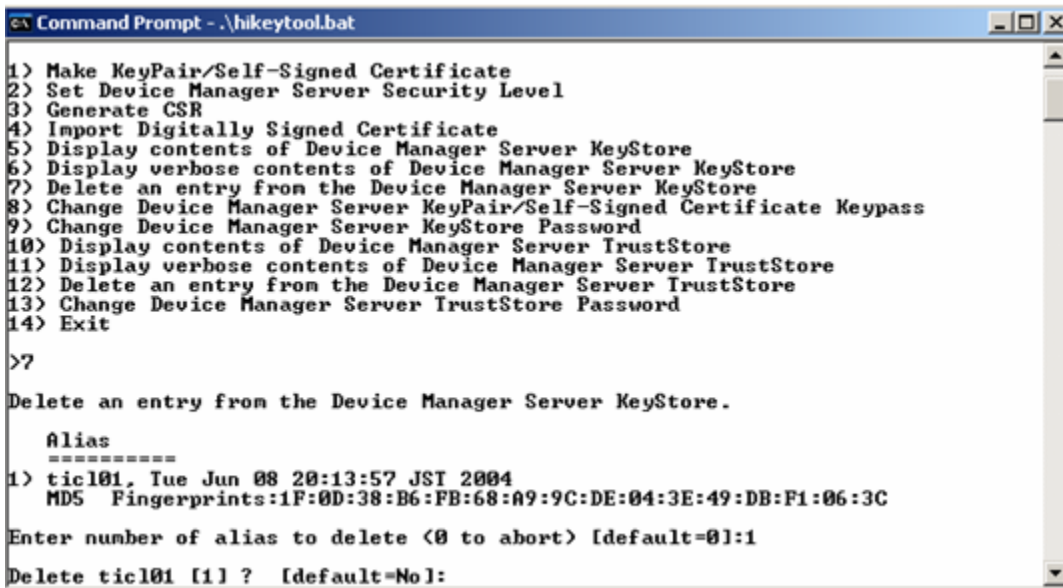
>7

Delete an entry from the Device Manager Server KeyStore.

Alias
=====
1) ticl01, Thu Mar 24 13:41:45 JST 2005
MD5 Fingerprints:32:EF:24:64:B1:65:42:4C:C3:E8:D1:27:FA:D4:1C:C2

Enter number of alias to delete (0 to abort) [default=0]:
```

Figure 7.13 Entering the Number of Alias to be Deleted



```
Command Prompt - .\hikeytool.bat
1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

>7

Delete an entry from the Device Manager Server KeyStore.

Alias
=====
1) ticl01, Tue Jun 08 20:13:57 JST 2004
MD5 Fingerprints:1F:0D:38:B6:FB:68:A9:9C:DE:04:3E:49:DB:F1:06:3C

Enter number of alias to delete (0 to abort) [default=0]:1

Delete ticl01 [1] ? [default=No]:
```

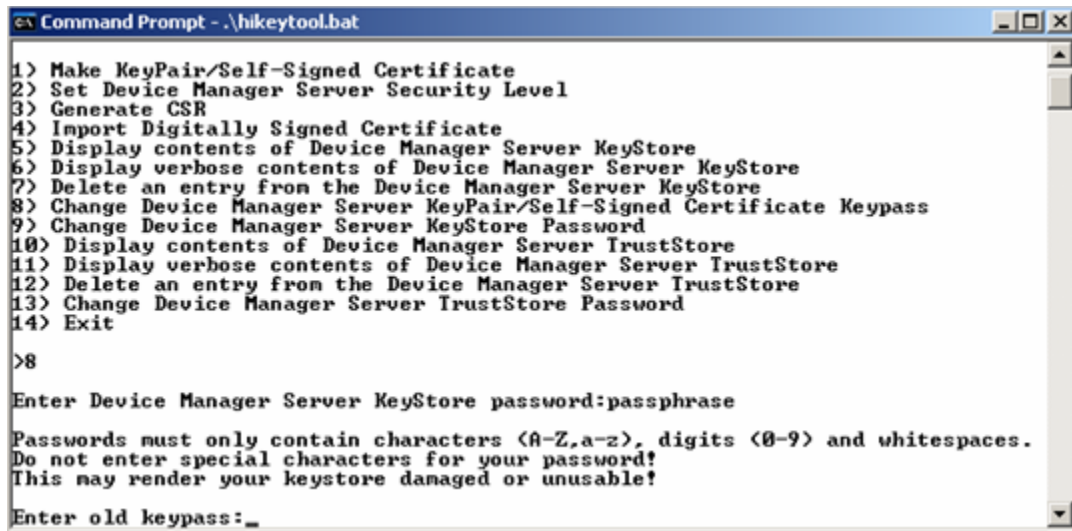
Figure 7.14 Confirming Deletion of an Alias

7.2.6 Changing the Device Manager Server Keypass

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 8 (**Change Device Manager Server Keypair/Self-Signed Certificate Keypass**).
3. Enter the existing HiCommand Device Manager server keystore password (see Figure 7.15).
4. Type the existing keypass and press **Enter** (see Figure 7.16).
5. Type the new keypass and press **Enter** (see Figure 7.17). This is case sensitive.
WARNING: Make sure to enter only characters (A-Z, a-z), numbers (0-9) or white space, or you can render your keystore unusable.
6. You will be prompted for a confirmation of the new Keypass. Type the new Keypass again and press **Enter** (see Figure 7.17).
7. You must restart the Device Manager server for the changes to be effective.



Figure 7.15 Entering the Current Keystore Password



```
Command Prompt - .\hikeytool.bat

1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

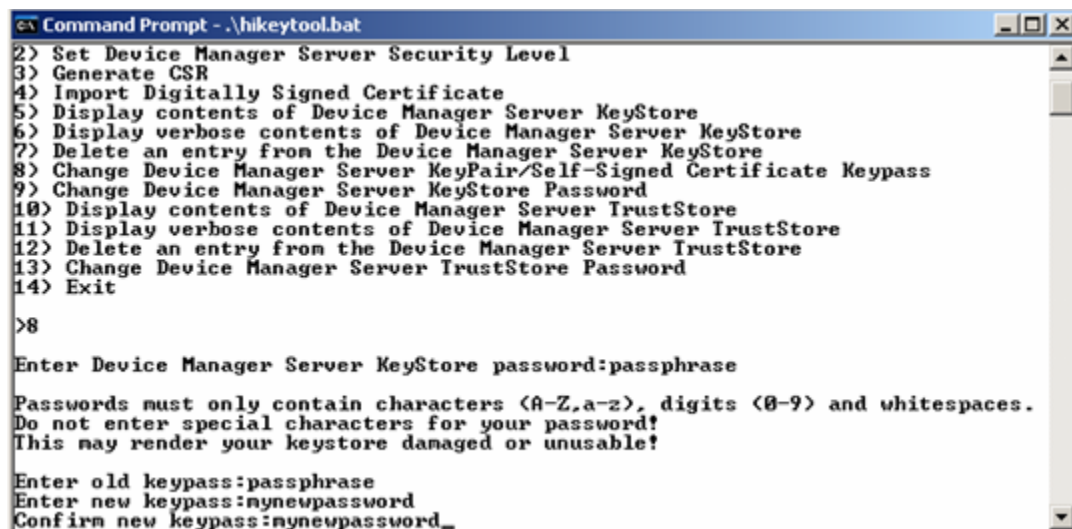
>8

Enter Device Manager Server KeyStore password:passphrase

Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old keypass:_
```

Figure 7.16 Entering the Old Keypass



```
Command Prompt - .\hikeytool.bat

2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

>8

Enter Device Manager Server KeyStore password:passphrase

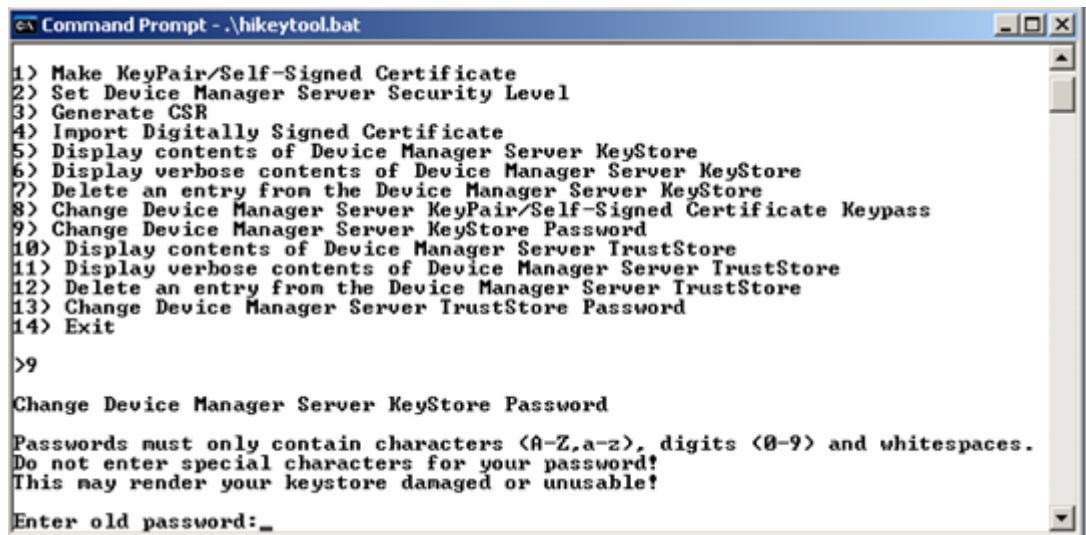
Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old keypass:passphrase
Enter new keypass:mynewpassword
Confirm new keypass:mynewpassword_
```

Figure 7.17 Entering and Confirming the New Keypass

7.2.7 Changing the Device Manager Server Keystore Password

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 9 (**Change Device Manager Server Keystore Password**).
3. Type the current keystore password, then press **Enter** (see Figure 7.18).
You will be prompted for your new password. (see Figure 7.19).
4. Type the new password and press **Enter** (see Figure 7.20).
This password is case-sensitive.
WARNING: Make sure to enter only characters (A-Z, a-z), numbers (0-9) or white space, or you can render your keystore unusable.
5. Confirm the new password (see Figure 7.20).
6. You will have to restart the Device Manager server for the changes to be effective.



```
Command Prompt - .\hikeytool.bat

1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server Keystore Password
10) Display contents of Device Manager Server TrustStore
11) Display verbose contents of Device Manager Server TrustStore
12) Delete an entry from the Device Manager Server TrustStore
13) Change Device Manager Server TrustStore Password
14) Exit

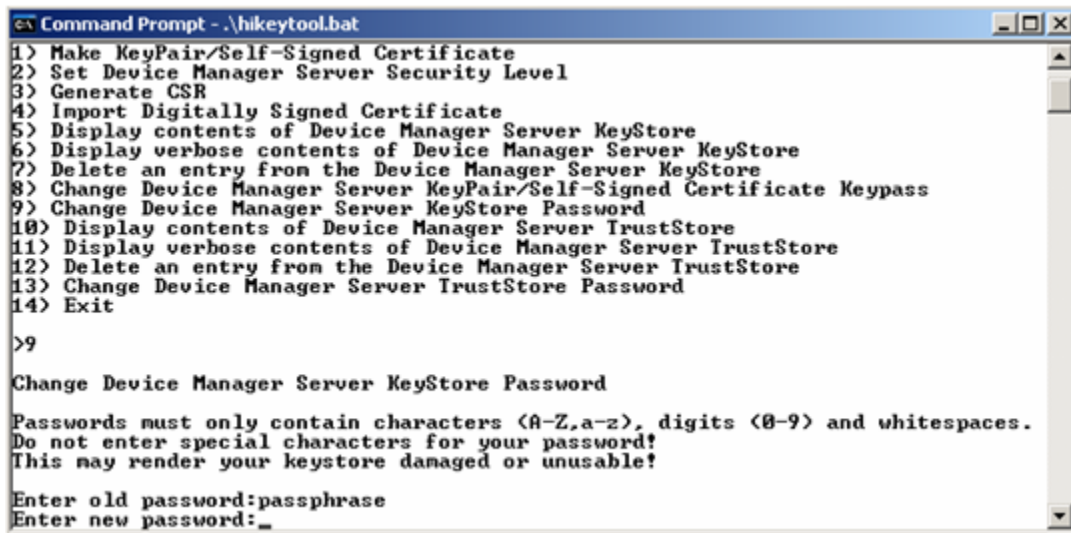
>9

Change Device Manager Server Keystore Password

Passwords must only contain characters <A-Z,a-z>, digits <0-9> and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old password: _
```

Figure 7.18 Entering Old Keystore Password



```
Command Prompt - .\hikeytool.bat
1> Make KeyPair/Self-Signed Certificate
2> Set Device Manager Server Security Level
3> Generate CSR
4> Import Digitally Signed Certificate
5> Display contents of Device Manager Server KeyStore
6> Display verbose contents of Device Manager Server KeyStore
7> Delete an entry from the Device Manager Server KeyStore
8> Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9> Change Device Manager Server KeyStore Password
10> Display contents of Device Manager Server TrustStore
11> Display verbose contents of Device Manager Server TrustStore
12> Delete an entry from the Device Manager Server TrustStore
13> Change Device Manager Server TrustStore Password
14> Exit

>9

Change Device Manager Server KeyStore Password

Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old password:passphrase
Enter new password:_
```

Figure 7.19 Entering New Keystore Password



```
Command Prompt - .\hikeytool.bat
2> Set Device Manager Server Security Level
3> Generate CSR
4> Import Digitally Signed Certificate
5> Display contents of Device Manager Server KeyStore
6> Display verbose contents of Device Manager Server KeyStore
7> Delete an entry from the Device Manager Server KeyStore
8> Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9> Change Device Manager Server KeyStore Password
10> Display contents of Device Manager Server TrustStore
11> Display verbose contents of Device Manager Server TrustStore
12> Delete an entry from the Device Manager Server TrustStore
13> Change Device Manager Server TrustStore Password
14> Exit

>9

Change Device Manager Server KeyStore Password

Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

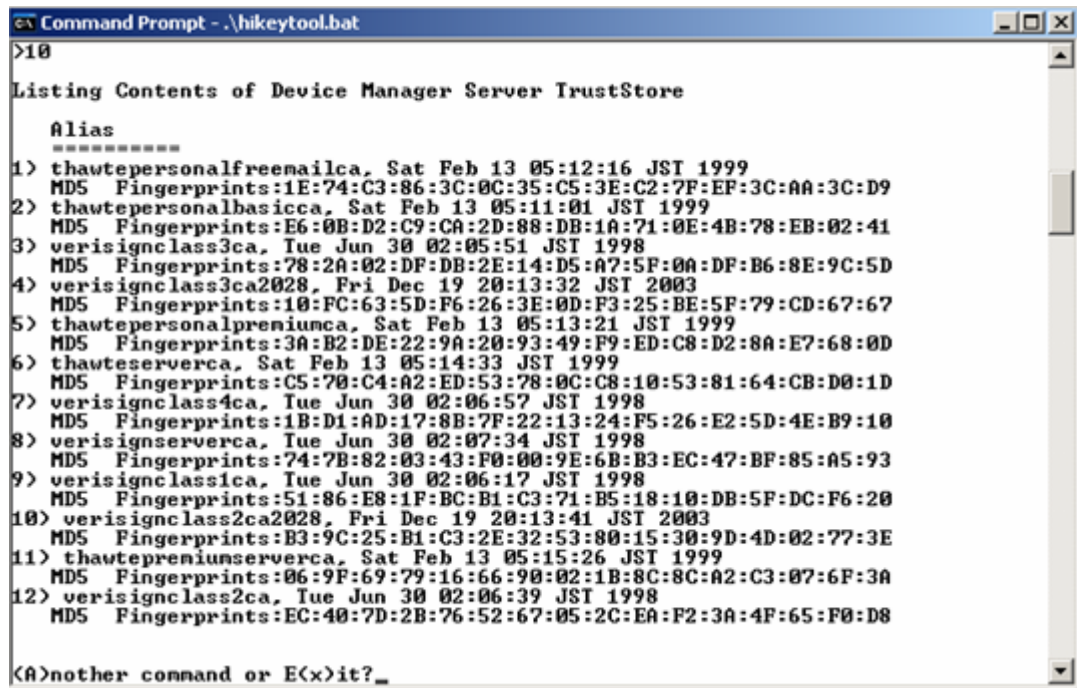
Enter old password:passphrase
Enter new password:mynewpassword
Confirm new password:_
```

Figure 7.20 Confirming New Keystore Password

7.2.8 Displaying Contents of HiCommand Device Manager Server Truststore

7.2.8.1 Regular Mode

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 10 (**Display Contents of Device Manager Server Truststore**).
3. The display will include the entry alias, the date the certificate was created, and the MD5 Fingerprints for that entry (see Figure 7.21).



```
Command Prompt - \\.\\hikeytool.bat
>10
Listing Contents of Device Manager Server TrustStore
Alias
=====
1) thawtepersonalfreemailca, Sat Feb 13 05:12:16 JST 1999
MD5 Fingerprints:1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
2) thawtepersonalbasicca, Sat Feb 13 05:11:01 JST 1999
MD5 Fingerprints:E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
3) verisignclass3ca, Tue Jun 30 02:05:51 JST 1998
MD5 Fingerprints:78:2A:02:DF:DB:2E:14:D5:A7:5F:0A:DF:B6:8E:9C:5D
4) verisignclass3ca2028, Fri Dec 19 20:13:32 JST 2003
MD5 Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
5) thawtepersonalpremiumca, Sat Feb 13 05:13:21 JST 1999
MD5 Fingerprints:3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D
6) thawteserverca, Sat Feb 13 05:14:33 JST 1999
MD5 Fingerprints:C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
7) verisignclass4ca, Tue Jun 30 02:06:57 JST 1998
MD5 Fingerprints:1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
8) verisignserverca, Tue Jun 30 02:07:34 JST 1998
MD5 Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
9) verisignclassica, Tue Jun 30 02:06:17 JST 1998
MD5 Fingerprints:51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20
10) verisignclass2ca2028, Fri Dec 19 20:13:41 JST 2003
MD5 Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E
11) thawtepersonalunserverca, Sat Feb 13 05:15:26 JST 1999
MD5 Fingerprints:06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
12) verisignclass2ca, Tue Jun 30 02:06:39 JST 1998
MD5 Fingerprints:EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8
<A>nother command or E<x>it?_
```

Figure 7.21 Contents of Device Manager Server Truststore

7.2.8.2 Verbose Mode

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 11 (**Display Verbose Contents of Device Manager Server Truststore**).
3. This will display the verbose information for each entry in the Device Manager Server truststore (see Figure 7.22).



```
Command Prompt - .\hikeytool.bat
Certificate: VALID
MD5 Fingerprints: 06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
SHA1 Fingerprints: 62:7F:8D:78:27:65:63:99:D2:7D:7F:90:44:C9:FE:B3:F3:3E:FA:9A

12>
alias: verisignclass2ca
Issued by: "VeriSign, Inc."
Organizational Unit: Class 2 Public Primary Certification Authority
Organization: "VeriSign, Inc."
Country: US
Created: Tue Jun 30 02:06:39 JST 1998
Entry Type: Trusted Certificate
Certificate Version: 1
Serial Number: ba5ac94c053b92d6a7b6df4ed053920d
Valid from: Mon Jan 29 09:00:00 JST 1996
Valid to: Thu Jan 08 08:59:59 JST 2004
Certificate: EXPIRED
MD5 Fingerprints: EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8
SHA1 Fingerprints: A5:EC:73:D4:8C:34:FC:BE:F1:00:5A:EB:85:84:35:24:BB:FA:B7:27

<A>nother command or E<x>it?
```

Figure 7.22 Displaying Verbose Information for Device Manager Truststore

7.2.9 Deleting an Entry from HiCommand Device Manager Server Truststore

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 12 (Delete an Entry from the Device Manager Server Truststore).
3. HiKeytool will display a list of all entries in the Device Manager Server truststore.
4. Type the number of the alias to be deleted from the Device Manager Server truststore, and press **Enter** (see Figure 7.23).
5. HiKeytool will request confirmation from the user to delete the designated entry. Enter Y to delete the entry (see Figure 7.24).
6. HiKeytool will delete the nominated entry, re-list the contents of the Device Manager Server truststore, and note that the deletion has been completed.

```

>12
Delete an entry from the Device Manager Server TrustStore.

Alias
=====
1> thawtepersonalfreemailca, Sat Feb 13 05:12:16 JST 1999
MD5 Fingerprints:1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
2> thawtepersonalbasicca, Sat Feb 13 05:11:01 JST 1999
MD5 Fingerprints:E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
3> verisignclass3ca, Tue Jun 30 02:05:51 JST 1998
MD5 Fingerprints:78:2A:02:DF:DB:2E:14:D5:A7:5F:0A:DF:B6:8E:9C:5D
4> verisignclass3ca2028, Fri Dec 19 20:13:32 JST 2003
MD5 Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
5> thawtepersonalpremiumca, Sat Feb 13 05:13:21 JST 1999
MD5 Fingerprints:3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D
6> thawteserverca, Sat Feb 13 05:14:33 JST 1999
MD5 Fingerprints:C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
7> verisignclass4ca, Tue Jun 30 02:06:57 JST 1998
MD5 Fingerprints:1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
8> verisignserverca, Tue Jun 30 02:07:34 JST 1998
MD5 Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
9> verisignclass1ca, Tue Jun 30 02:06:17 JST 1998
MD5 Fingerprints:51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20
10> verisignclass2ca2028, Fri Dec 19 20:13:41 JST 2003
MD5 Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E
11> thawtepremiumserverca, Sat Feb 13 05:15:26 JST 1999
MD5 Fingerprints:06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
12> verisignclass2ca, Tue Jun 30 02:06:39 JST 1998
MD5 Fingerprints:EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8

Enter number of alias to delete (0 to abort) [default=0]:_

```

Figure 7.23 Entering the Alias to be Deleted from Truststore

```

Command Prompt - .\hikeytool.bat
6> MD5 Fingerprints:3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D
thawteserverca, Sat Feb 13 05:14:33 JST 1999
MD5 Fingerprints:C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
7> verisignclass4ca, Tue Jun 30 02:06:57 JST 1998
MD5 Fingerprints:1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
8> verisignserverca, Tue Jun 30 02:07:34 JST 1998
MD5 Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
9> verisignclass1ca, Tue Jun 30 02:06:17 JST 1998
MD5 Fingerprints:51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20
10> verisignclass2ca2028, Fri Dec 19 20:13:41 JST 2003
MD5 Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E
11> thawtepremiumserverca, Sat Feb 13 05:15:26 JST 1999
MD5 Fingerprints:06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
12> verisignclass2ca, Tue Jun 30 02:06:39 JST 1998
MD5 Fingerprints:EC:40:7D:2B:76:52:67:05:2C:EA:F2:3A:4F:65:F0:D8

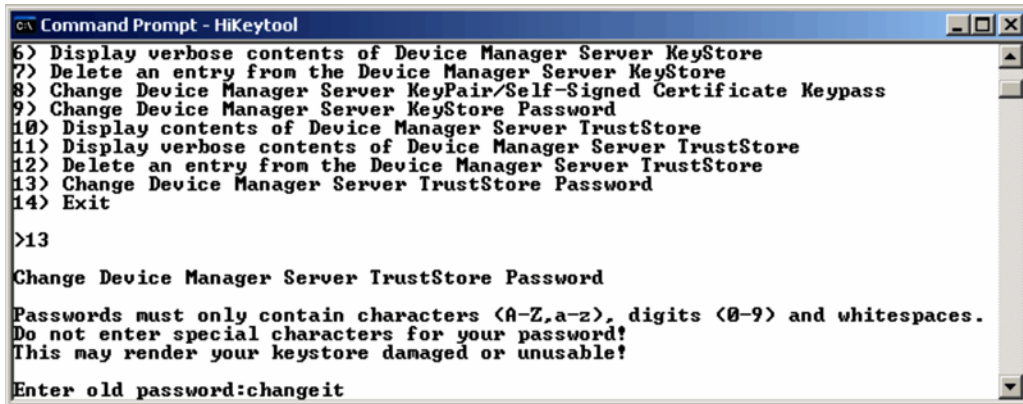
Enter number of alias to delete (0 to abort) [default=0]:1
Delete thawtepersonalfreemailca [1] ? [default=No]:y_

```

Figure 7.24 Confirming the Alias to be Deleted From Truststore

7.2.10 Changing the HiCommand Device Manager Server Truststore Password

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 13 (Change Device Manager Server Truststore Password).
3. Type the existing truststore password and press **Enter** (see Figure 7.25).
The truststore password will be set in the `server.https.truststore.passphrase` property of the Device Manager server properties file. (For details, see section 8.8.9.)
4. Type the new truststore password and press **Enter** (see Figure 7.26). This password is case sensitive.
WARNING: Make sure to enter only characters (A-Z, a-z), numbers (0-9) or white space, or you can render your keystore unusable.
5. Type the new password in again, and press **Enter** (see Figure 7.26).
6. You will need to restart the Device Manager server for the changes to take effect.



```
Command Prompt - HiKeytool
6> Display verbose contents of Device Manager Server KeyStore
7> Delete an entry from the Device Manager Server KeyStore
8> Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9> Change Device Manager Server KeyStore Password
10> Display contents of Device Manager Server TrustStore
11> Display verbose contents of Device Manager Server TrustStore
12> Delete an entry from the Device Manager Server TrustStore
13> Change Device Manager Server TrustStore Password
14> Exit

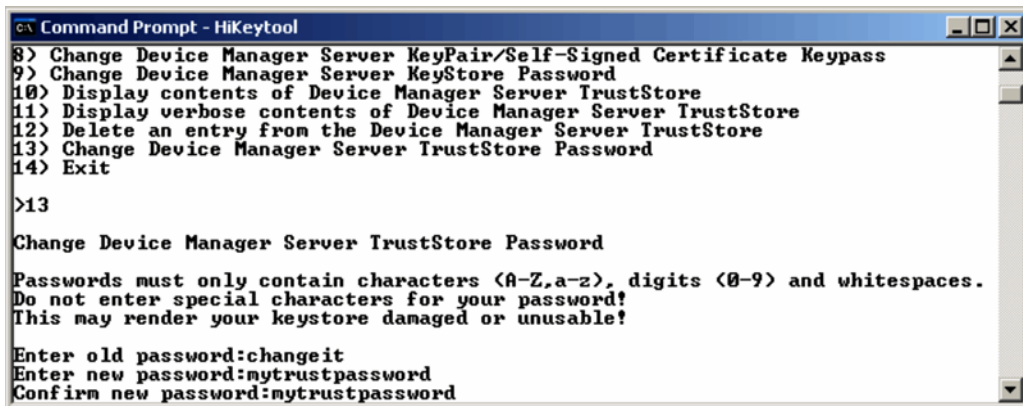
>13

Change Device Manager Server TrustStore Password

Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old password:changeit
```

Figure 7.25 Entering the Current Truststore Password



```
Command Prompt - HiKeytool
8> Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9> Change Device Manager Server KeyStore Password
10> Display contents of Device Manager Server TrustStore
11> Display verbose contents of Device Manager Server TrustStore
12> Delete an entry from the Device Manager Server TrustStore
13> Change Device Manager Server TrustStore Password
14> Exit

>13

Change Device Manager Server TrustStore Password

Passwords must only contain characters (A-Z,a-z), digits (0-9) and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter old password:changeit
Enter new password:mytrustpassword
Confirm new password:mytrustpassword
```

Figure 7.26 Entering and Confirming New Truststore Password

7.3 Configuring the HBase Storage Management Web Service for SSL

The HBase Storage Mgmt Web Service supports versions 3 of SSL, and version 1 of TLS.

This section discusses the following security procedures:

- Generating a Private Key (see section 7.3.1)
- Creating a Certificate Signing Request (CSR) (see section 7.3.2)
- Creating a Self-Signed Certificate (see section 7.3.3)
- Enabling SSL (see section 7.3.4.1)
- Disabling SSL (see section 7.3.4.2)
- Changing a Port Assigned to SSL (see section 7.3.4.3)

This section gives notes on setting SSL (see section 7.3.5).

7.3.1 Generating a Private Key Using SSLC

To create a private key, you will use the `sslc` utility. You can either use the private key as the basis for a certificate signing request (see section 7.3.2), or you can use it as a self-signed certificate to test the web server. The default location of the `sslc` utility is as follows:

Windows:

`C:\Program Files\HiCommand\Base\httpd\sslc\bin`

Solaris or Linux:

`/opt/HiCommand/Base/httpd/sslc/bin`

The `sslc` utility has the following format:

`sslc genrsa -out key-file [ 512 | 1024 | 2048 ]`

- `out key-file` specifies the file that will contain the private key.
- `[ 512 | 1024 | 2048 ]` specifies the bit length of the private key.

For example, to output a 1024-bit private key to the `httpsdkey.pem` file, the command would be:

- `# .\sslc genrsa -out demoCA/httpsdkey.pem 1024` (Windows)
- `# ./sslc genrsa -out demoCA/httpsdkey.pem 1024` (Solaris)

This would generate the following output:

```
1160 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
```

Figure 7.27 Output of # ./sslc genrsa -out demoCA/httpsdkey.pem 1024 Command

7.3.2 Creating a Certificate Signing Request (CSR)

Use the sslc req utility to create a Certificate Signing Request (CSR), which you will send to a Certificate Authority (CA). The CA will send you a signed certificate. The exact format of the CSR will vary depending on which CA you use.

The default location of the sslc req utility is as follows:

Windows:

C:\Program Files\HiCommand\Base\httpsd\sslc\bin\demoCA

Solaris or Linux:

/opt/HiCommand/Base/httpsd/sslc/bin/ demoCA

The sslc req utility has the following format:

sslc req -config configuration-file -new -key key-file -out CSR-file

- **-config configuration-file** specifies the sslc.cnf file that contains the information you want the utility to access. When you define information in the sslc.cnf file in advance, you do not need to enter information such as Country Name and Locality Name on the command line. If you want to use information that is different than previously defined, you need to specify it when prompted.
- **-new** indicates a new CSR (required).
- **-key key-file** indicates the file containing the private key.
- **-out CSR-file** indicates the file that will contain the Certificate Signing Request (CSR).

For example, to output a CSR when the configuration file is demoCA/sslc.cnf, the key file is demoCA/httpsdkey.pem, and the name of the CSR file is demoCA/httpsd.csr, the command would be:

- # ./sslc req -config demoCA/sslc.cnf -new -key demoCA/httpsdkey.pem -out demoCA/httpsd.csr (Windows)
- # ./sslc req -config demoCA/sslc.cnf -new -key demoCA/httpsdkey.pem -out demoCA/httpsd.csr (Solaris)

The utility would prompt you to enter certain information, including the country name and locality. If you want to leave a field blank, enter a period (.). If you want to select the default, press **Enter**.

Note: For Common Name, specify the host name of the web server. The prompts appear generally as follows:

```
You will be prompted to enter information to incorporate into the certificate request.
This information is called a Distinguished Name or a DN.
There are many fields however some can remain blank.
Some fields have default values.
Enter '.', to leave the field blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:Washington
Locality Name (eg, city) []:New York
Organization Name (eg, company) []:HITACHI
Organizational Unit Name (eg, section) []:WebSite
Common Name (eg, YOUR name) []:www.example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Figure 7.28 sslc req Utility Prompts

7.3.3 Creating a Self-Signed Certificate

If you do not have a signed and trusted certificate, you can create a self-signed certificate using the `sslc x509` utility. This is useful if you want to test the web server.

The `sslc x509` utility has the following format:

- `sslc x509 -in CSR-file -out certificate-file -req -signkey key-file -days valid-period.`
- `-in CSR-file` specifies the Certificate Signing Request (CSR) file to be passed to the utility.
- `-out certificate-file` specifies the file for containing the created self-signed certificate.
- `-req` indicates the request (required).
- `-signkey key-file` specifies the file that contains the private key.
- `-days valid-period` specifies the number of days during which the self-signed certificate is valid.

For example, to create a private key when the CSR file is `demoCA/httpsd.csr`, the key file is `demoCA/httpsdkey.pem`, and the name of the file that will contain the self-signed certificate is `demoCA/newcert.pem`, the command would be:

- **# `./sslc x509 -in demoCA/httpsd.csr -out demoCA/newcert.pem -req -signkey demoCA/httpsdkey.pem -days 365` (Windows).**
- **# `./sslc x509 -in demoCA/httpsd.csr -out demoCA/newcert.pem -req -signkey demoCA/httpsdkey.pem -days 365` (Solaris).**

This would create the following output:

Signature OK subject=/C=US/ST=Washington/L=New York/O=HITACHI/OU=WebSite/CN=www.example.com
--

Figure 7.29 Sample Output of a `sslc x509` Command

7.3.4 Configuring SSL

7.3.4.1 Enabling SSL

To enable SSL:

1. Stop any other HiCommand Suite Common Component that is running.
2. Stop the Device Manager and HiCommand Suite Common Component.
 - In Windows
From **Start**, choose **Programs, HiCommand, Device Manager**, and then **Stop Server with Common Services**
 - In Solaris or Linux
Execute the following command:

```
# /opt/HiCommand/suitesrvctl -stop_all
```
3. Open the httpsd.conf file.
4. Make the directives for the SSL port and logical host effective by deleting the pound sign (#) at the beginning of the corresponding lines.
5. Specify the full path name of the certificate file received from the Certificate Authority .
6. SSLCertificateFile directive
7. Specify the full path name of the private key file for the Web server.
8. SSLCertificateKeyFile directive
9. Specify the full path name of the certificate file of the chained Certificate Authority.
10. SSLCACertificateFile directive.
Note: If the certificate file from a Certificate Authority has not been distributed, you do not need to set this directive.
11. Start the Device Manager and HiCommand Suite Common Component.
 - In Windows
From **Start**, choose **Programs, HiCommand, Device Manager**, and then **Stop Server with Common Services**
 - In Solaris or Linux
Execute the following command:

```
# /opt/HiCommand/suitesrvctl -start_all
```

Caution: Set the SSLCACertificateFile directive only when you use a server certificate issued by a chained Certificate Authority.

Figure 7.30 is an example of enabling SSL in Windows, where the signed certificate (httpsd.pem) received from a CA and the private key (httpsdkey.pem) are placed in the folder **c:\ProgramFiles\HiCommand\Base\httpsd\conf\ssl\server**.

Note: The line that begins with a pound sign (#) is a comment line.

```
Listen 23015
SSLDisable

Listen 23016
<VirtualHost www.example.com:23016>
  ServerName www.example.com
  SSLEnable
  SSLRequireSSL
  SSLCertificateFile "c:/Program Files/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem"
  SSLCertificateKeyFile "c:/Program
Files/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem"
# SSLCACertificateFile "c:/Program Files/HiCommand/Base/httpsd/conf/ssl/cacert
/anycert.pem"
  SSLSessionCacheTimeout 3600
</VirtualHost>
```

Figure 7.30 Enabling SSL (Windows)

Figure 7.31 is an example of enabling SSL in Solaris or Linux, where the signed certificate (httpsd.pem) received from a CA and the private key (httpsdkey.pem) are placed in the directory /opt/HiCommand/Base/httpsd/conf/ssl/server .

Note: The line that begins with a pound sign (#) is a comment line.

```
Listen 23015
SSLDisable

Listen 23016
<VirtualHost www.example.com:23016>
    ServerName www.example.com
    SSLEnable
    SSLRequireSSL
    SSLCertificateFile /opt/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem
    SSLCertificateKeyFile /opt/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem
    # SSLCACertificateFile /opt/HiCommand/Base/httpsd/conf/ssl/cacert/anycert.pem
    SSLSessionCacheTimeout 3600
</VirtualHost>
SSLCacheServerPort /opt/HiCommand/Base/httpsd/logs/gcache_port
SSLCacheServerPath /opt/HiCommand/Base/httpsd/sbin/gcache
SSLCacheServerRunDir /opt/HiCommand/Base/httpsd/logs
```

Figure 7.31 Enabling SSL (Solaris or Linux)

7.3.4.2 Disabling SSL

To disable SSL, comment out the directives for the SSL port and **logical** host in the httpsd.conf file.

Caution: Stop the Device Manager and HiCommand Suite Common Component, and then edit the httpsd.conf file. After editing the file, start the Device Manager and HiCommand Suite Common Component to apply the changes.

Figure 7.32 is an example of disabling SSL in Windows.

Note: The line that begins with a pound sign (#) is a comment line.

```
Listen 23015
SSLDisable

#Listen 23016
#<VirtualHost www.example.com:23016>
# ServerName www.example.com
# SSLEnable
# SSLRequireSSL
# SSLCertificateFile "c:/Program Files/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem"
# SSLCertificateKeyFile "c:/Program
Files/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem"
# SSLCACertificateFile "c:/Program Files/HiCommand/Base/httpsd/conf/ssl/cacert
/anycert.pem"
# SSLSessionCacheTimeout 3600
#</VirtualHost>
```

Figure 7.32 Disabling SSL (Windows)

Figure 7.33 is an example of disabling SSL in Solaris or Linux.

Note: The line that begins with a pound sign (#) is a comment line.

```
Listen 23015
SSLDisable

#Listen 23016
#<VirtualHost www.hws.hitachi.co.jp:23016>
#  ServerName www.hws.hitachi.co.jp
#  SSLEnable
#  SSLRequireSSL
#  SSLCertificateFile /opt/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem
#  SSLCertificateKeyFile /opt/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem
#  SSLCACertificateFile /opt/HiCommand/Base/httpsd/conf/ssl/cacert/anycert.pem
#  SSLSessionCacheTimeout 3600
#</VirtualHost>
# SSLCacheServerPort /opt/HiCommand/Base/httpsd/logs/gcache_port
# SSLCacheServerPath /opt/HiCommand/Base/httpsd/sbin/gcache
# SSLCacheServerRunDir /opt/HiCommand/Base/httpsd/logs
```

Figure 7.33 Disabling SSL (Solaris or Linux)

7.3.4.3 Changing a Port Assigned to SSL

The default port of SSL for HBase Storage Mgmt Web Service is 23016. To change the port, edit the httpsd.conf file and hssso.conf file.

Caution: Stop the Device Manager and HiCommand Suite Common Component, and then edit the httpsd.conf file and hssso.conf file. After editing these files, start the Device Manager and HiCommand Suite Common Component to apply the changes.

7.3.5 About Setting SSL

Caution: When SSL communication is set for Device Manager, it can be used between the HBase Storage Mgmt Web Service and the Device Manager server, and between the Device Manager server and the Web Client. For details about SSL settings for linked applications, see the appropriate documentation.

When you set SSL, you will need to specify a logical host name for the cluster manager IP address. That IP address must be enabled and accessible. If that IP address was specified during Device Manager installation, execute the following command:

Windows:

```
c:\Program Files\HiCommand\Base\bin\hcmdschgurl -change http://<cluster manager IP address>:port number http://<host name for the cluster manager IP address>:port number
```

Solaris:

```
# /opt/HiCommand/Base/bin/hcmdschgurl /change http:// <cluster manager IP address>:port number http:// <host name for the cluster manager IP address>:port number
```

7.3.5.1 Security Settings for HiCommand Device Manager Server

If you are creating a keypair by using HiKeytool, specify a logical host name in **Enter Server Name[default=HDM_Server]**: (see Figure 7.3).

7.3.5.2 SSL Settings for HBase Storage Mgmt Web Service

When creating a Certificate Signing Request (CSR), specify an IP address for cluster management and a logical host name in Common Name (eg, YOUR name). That IP address must be enabled and accessible.

If you are editing the **httpsd.conf** file, you must specify the virtual host name for **VirtualHost** and a logical host name in **ServerName**.

Figure 7.34 shows the editing format for the **httpsd.conf** file.

```
#Listen 23016
<VirtualHost virtual-host-name:port-number>
  ServerName logical-host-name
  SSLEnable
  SSLRequireSSL
  SSLCertificateFile signed-certificate-file
  SSLCertificateKeyFile private-key-file-for-the-Web-server
  SSLCACertificateFile certificate-file-of-chained-authorized-body
  SSLSessionCacheTimeout 3600
</VirtualHost>
```

Figure 7.34 Editing Format for the httpsd.conf File

Caution: Stop the Device Manager and HiCommand Suite Common Component, and then edit the `httpsd.conf` file. After editing the file, start the Device Manager and HiCommand Suite Common Component to apply the changes.

7.4 Security Settings for CIM/WBEM Functionality

CIM/WBEM functionality supports SSL communication for the following functions:

- Object operations

In the object operation feature, a CIM client acts as an SSL client and the Device Manager server acts as an SSL server.

By default, you can perform SSL communication in object operations. If you want to modify a keystore file used for SSL, see section 7.4.1.

- Event indication

In the event indication feature, the Device Manager server acts as an SSL client and a CIM client (Indication Listener) acts as an SSL server.

By default, the Device Manager server can use SSL communication to receive event indications by following the CIM client requests. In this case, settings must be specified beforehand to enable SSL communication between the CIM clients.

In addition, you can strengthen security by applying two-way authentication for object operations and event indication. Two-way authentication enables communications between pre-specified trusted users. In this way, users can accept object operations from specific CIM clients only, and send event indications to specific CIM clients only. For details on the setting procedures, see section 7.4.2 and 7.4.3.

Caution: You must enable CIM/WBEM functionality to perform SSL communication. For details on setting up CIM/WBEM features, see Chapter 11.

Note: Use Java™ commands to set up SSL, as described in section 7.5.

7.4.1 Modifying the Keystore File for Object Operations

The keystore file used for CIMOM object operations (the keystore password is `wbemssl`) is by default stored in the following location and can be used without any modification:

In Windows:

```
installation-folder-for-the-Device-Manager-  
Server\HiCommandServer\wsi\server\jserver\bin\.keystore
```

In Solaris or Linux:

```
/opt/HiCommand/HiCommandServer/wsi/server/jserver/bin/.keystore
```

To modify the keystore file:

1. Create a keystore file. Name the file `.keystore` and use it to replace the default keystore file. For details on how to create a keystore file, see section 7.5.1.
2. Encrypt the keystore password.

Use `WSEncryptString.jar` to encrypt the keystore password that was specified during creation of the keystore file in step 1. `WSEncryptString.jar` is stored in the following location:

- In Windows:

*installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\no-redis*t

- In Solaris or Linux:

*/opt/HiCommand/HiCommandServer/wsi/no-redis*t/

Example of executing the command:

> java -jar WSEncryptString.jar keystore-password

When the command is executed, the encrypted character string of the keystore password is displayed. This character string is used in a later step.

3. Stop the Device Manager server.

- In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.

- In Solaris or Linux:

Execute the following command:

/opt/HiCommand/suitesrvctl -stop_hdvm

4. Modify the MOF file (`WBEMSolutions_CIMXMLCPA.mof`).

Specify in the MOF file the keystore password that was encrypted in step 2 of this procedure. The MOF file is stored in the following location:

- In Windows:

installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\mof

- In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/server/jserver/mof

```
instance of WBEMSolutions_HttpsCPASettingData as $d {
InstanceID = "WBEMSolutions:WBEMSolutions_HttpsCPASettingData:001";
ElementName = "WBEM Solutions HTTPS Client Adapter Settings";
ClientAuthenticationEnabled = false;
ServerKeyStorePassword = "xxxxxx";
};
```

Figure 7.35 MOF File Example

The `xxxxxxx` part of `ServerKeyStorePassword` contains the character string that encrypted the keystore password used by the default keystore file. In `xxxxxxx`, specify the keystore password that you encrypted in step 2.

5. Compile the MOF file.

Use the `mofcomp` command to compile the MOF file. The `mofcomp` command is stored in the following location:

- In Windows:

```
installation-folder-for-the-Device-Manager-  
Server\HiCommandServer\wsi\bin\mofcomp.bat
```

- In Solaris or Linux:

```
/opt/HiCommand/HiCommandServer/wsi/bin/mofcomp
```

Example of executing the command:

```
> mofcomp -s http://localhost/interop -SI -o ..\server\jserver\logr  
..\server\jserver\mof\WBEMSolutions_CIMXMLCPA.mof
```

6. Start the Device Manager Server.

Start the Device Manager server as follows:

- In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Start Server**.

- In Solaris or Linux:

Execute the following command:

```
# /opt/HiCommand/suitesrvctl -start_hdvm
```

7.4.2 Specifying Two-Way Authentication for Object Operations

This section describes how to set up two-way authentication for object operations. Use HiKeytool for this task.

7.4.2.1 First Setup Procedure Performed in a CIM client

Create a keystore file for the CIM, and export the client authentication file.

For details on creating a keystore file, see section 7.5.1. For details on exporting an authentication file, see section 7.5.2.

7.4.2.2 Setup Procedure Performed in the Device Manager Server

The following describes the procedure for setting up two-way authentication, importing the client authentication file, and exporting the server authentication file.

1. Open a command prompt or terminal window, navigate to the *HiCommand-server-directory*, and run HiKeytool.
 - For Windows, type **HiKeytool.bat**, and then press the **Enter** key.
 - For Solaris or Linux, log on as the root user. Type **HiKeytool.sh** and press the **Enter** key.

2. The HiKeytool main panel appears (see Figure 7.1). Enter 2.

The SMI-S main panel appears as in the example shown below.

```
1) Set Security Level for Object Operations
(Current setting:SSL without two-way authentication)
2) Set Security Level for Event Indications
(Current setting:SSL without two-way authentication)
3) Import Client's Certificate to TrustStore for Object Operations
4) Import Client's Certificate to TrustStore for Event Indications
5) Export Server's Certificate from KeyStore for Object Operations
6) Export Server's Certificate from KeyStore for Event Indications
7) Exit
>
```

3. If (Current setting:SSL without two-way authentication) appears at item 1 in the SMI-S main panel, type 1.

If (Current setting:SSL with two-way authentication) appears in the SMI-S main panel, skip to step 6.

When you type 1 in the SMI-S main panel, a submenu appears as in the example shown below.

```
You must stop the Device Manager Server before specifying this setting.
1) SSL without two-way authentication
2) SSL with two-way authentication
>
```

4. Stop the Device Manager server as indicated in the displayed message.

Stop the Device Manager server as follows:

- In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.

- In Solaris or Linux:

Execute the following command:

```
# /opt/HiCommand/suitesrvctl -stop_hdvm
```

5. Type 2 in the submenu.

The `mofcomp` command is executed and the MOF file is compiled.

You are returned to the SMI-S main panel when the `mofcomp` command has completed execution.

Caution: If you type the same number as the current setting, you are immediately returned to the SMI-S main panel.

Caution: If `mofcomp` command execution fails, the following message appears: The compilation of the MOF file failed. In this case, collect all files in the following directory, and then contact maintenance personnel.

- In Windows:

```
installation-folder-for-the-Device-Manager-  
Server\HiCommandServer\wsi\server\jserver\mof
```

- In Solaris or Linux:

```
/opt/HiCommand/HiCommandServer/wsi/server/jserver/mof
```

6. In the SMI-S main panel, enter 3.

This option starts processing to import the client authentication file to the truststore file for object operations.

Note: The truststore file for object operations (the truststore password is `trustssl`) is stored in the following location:

- In Windows:

```
installation-folder-for-the-Device-Manager-  
Server\HiCommandServer\wsi\server\jserver\bin\.truststore
```

- In Solaris or Linux:

```
/opt/HiCommand/HiCommandServer/wsi/server/jserver/bin/.truststo  
re
```

7. Enter the alias, the truststore password, and the client authentication file name.

Enter the client authentication file name by absolute path.

An input example is shown below.

```
Enter alias:foocorpclient  
Enter truststore-password:trustssl  
Enter authentication-filename(absolute path):c:\tmp\client.cer
```

At completion of processing, you are returned to the SMI-S main panel.

8. In the SMI-S main panel, enter 5.

This option starts processing to export the server authentication file from the keystore file for object operations.

9. Enter the keystore password, the alias, and the server authentication file name.

Enter the server authentication file name by absolute path.

An input example is shown below.

```
Enter keystore-password: serverssl  
Enter alias: foocorpserver  
Enter authentication-filename (absolute path) : c:\tmp\server.cer
```

At completion of processing, you are returned to the SMI-S main panel.

10. Start the Device Manager server if stopped.

Start the Device Manager server as follows:

- In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Start Server**.

- In Solaris or Linux:

Execute the following command:

/opt/HiCommand/suitesrvctl -start_hdvm

7.4.2.3 Second Setup Procedure Performed in a CIM Client

Import the server authentication file for object operation into the truststore file for the CIM client.

For details on creating a truststore file and importing the authentication file, see section 7.5.3.

7.4.3 Procedure for Specifying Two-way Authentication for Event Indications

This section describes how to set up two-way authentication for event indications.

7.4.3.1 First Setup Procedure Performed in a CIM Client

Create a keystore file for the CIM and export the client authentication file.

For details on creating a keystore file, see section 7.5.1. For details on exporting an authentication file, see section 7.5.2.

7.4.3.2 Setup Procedure Performed in the Device Manager Server

The following describes the procedure for creating a keystore file and setting up two-way authentication for event indications, importing the client authentication file, and exporting the server authentication file.

1. Create a new keystore file for the event indication.

The default keystore file for the event indication (the keystore password is `indssl`) is stored in the following location:

- In Windows:

installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\bin\.ind.keystore

- In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/server/jserver/bin/.ind.keystore

The default keystore file can be used without any modification. If you want to use the default keystore file, skip to step 6.

If you want to create a new keystore file, name the file `.ind.keystore` and use it to replace the default keystore file.

For details on how to create a keystore file, see section 7.5.1.

2. Encrypt the keystore password.

Use `WSEncryptString.jar` to encrypt the keystore password that was specified during creation of the keystore file in step 1. `WSEncryptString.jar` is stored in the following location:

- In Windows:

installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\no-redis

- In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/no-redis/

Example of executing the command:

> java -jar WSEncryptString.jar keystore-password

When the command is executed, the encrypted character string of the keystore password is displayed. This character string is used in a later step.

3. Stop the Device Manager Server.

Stop the Device Manager server as follows:

- In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.

- In Solaris or Linux:

Execute the following command:

/opt/HiCommand/suitesrvctl -stop_hdvm

4. Modify the MOF file.

Specify, in the MOF file, the encrypted keystore password that was obtained in step 2 of this procedure. The MOF file is stored in the following location:

- In Windows:

installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\mof

- In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/server/jserver/mof

See Figure 7.35 for an example of a MOF file.

5. In the MOF file, change **IndicationAuthenticationEnabled** to **true**. Compile the MOF file.

Use the `mofcomp` command to compile the file. The `mofcomp` command is stored in the following location:

- In Windows:

installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\bin\mofcomp.bat

- In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/bin/mofcomp

6. Open a command prompt or terminal window, navigate to the *HiCommand-server-directory*, and run `HiKeytool`.

- For Windows, type **HiKeytool.bat**, and then press the **Enter** key.
- For Solaris or Linux, log on as the root user. Type **HiKeytool.sh** and press the **Enter** key.

7. The HiKeytool main panel appears (see Figure 7.1). Enter 2.

The SMI-S main panel appears.

```
1) Set Security Level for Object Operations
(Current setting:SSL without two-way authentication)
2) Set Security Level for Event Indications
(Current setting:SSL without two-way authentication)
3) Import Client's Certificate to TrustStore for Object Operations
4) Import Client's Certificate to TrustStore for Event Indications
5) Export Server's Certificate from KeyStore for Object Operations
6) Export Server's Certificate from KeyStore for Event Indications
7) Exit
>
```

8. If (Current setting:SSL without two-way authentication) appears at item 2 in the SMI-S main panel, type 2.

If (Current setting:SSL with two-way authentication) appears in the SMI-S main panel, skip to step 11.

When you type 2 in the SMI-S main panel, a submenu appears as in the example shown below.

```
You must stop the Device Manager Server before specifying this setting.
1) SSL without two-way authentication
2) SSL with two-way authentication
>
```

9. Stop the Device Manager server, if running, as indicated in the displayed message.

Stop the Device Manager server as follows:

- In Windows:
Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.
- In Solaris or Linux:
Execute the following command:

```
# /opt/HiCommand/suitesrvctl -stop_hdvm
```

10. Type 2 in the submenu.

The `mofcomp` command is executed and the MOF file is compiled.

You are returned to the SMI-S main panel when the `mofcomp` command has completed execution.

Caution: If you type the same number as the current setting, you are immediately returned to the SMI-S main panel.

Caution: If `mofcomp` command execution fails, the following message appears: The compilation of the MOF file failed. In this case, collect all files in the following directory, and then contact maintenance personnel.

- In Windows:

installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\mof

- In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/server/jserver/mof

11. In the SMI-S main panel, enter 4.

This option starts processing to import the client authentication file to the truststore file for event indications.

Important: The truststore file for the event indication (the truststore password is *indtrust*) is stored in the following location:

- In Windows:

installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\bin\.ind.truststore

- In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/server/jserver/bin/.ind.truststore

12. Enter the alias, the truststore password, and the client authentication file name.

Enter the client authentication file name by absolute path.

An input example is shown below.

```
Enter alias:foocorpindclient
Enter truststore-password:indtrust
Enter authentication-filename(absolute path):c:\tmp\clientind.cer
```

At completion of processing, you are returned to the SMI-S main panel.

13. In the SMI-S main panel, enter 6.

This option starts processing to export the server authentication file from the keystore file for event indications.

14. Enter the keystore password, the alias, and the server authentication file name.

Enter the server authentication file name by absolute path.

An input example is shown below.

```
Enter keystore-password:serverindtrust
Enter alias:foocorpindserver
Enter authentication-filename(absolute path):c:\tmp\serverind.cer
```

At completion of processing, you are returned to the SMI-S main panel.

15. Start the Device Manager server if stopped.

- In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Start Server**.

- In Solaris or Linux:

Execute the following command:

/opt/HiCommand/suitesrvctl -start_hdvm

7.4.3.3 Second Setup Procedure Performed in a CIM Client

Import the server authentication file for object operation into the truststore file for the CIM client.

For details on creating a truststore file and importing the authentication file, see section 7.5.3.

7.4.4 Procedure for Disabling Two-way Authentication

The procedure for disabling two-way authentication for object operations or event indications is described below. Use HiKeytool for this task.

1. Open a command prompt or terminal window, navigate to the *HiCommand-server-directory*, and run HiKeytool.
 - For Windows, type **HiKeytool.bat**, and then press the **Enter** key.
 - For Solaris or Linux, log on as the root user. Type **HiKeytool.sh** and press the **Enter** key.

2. The HiKeytool main panel appears (see Figure 7.1). Enter 2.

The SMI-S main panel appears as in the example shown below.

```
1) Set Security Level for Object Operations
(Current setting:SSL with two-way authentication)
2) Set Security Level for Event Indications
(Current setting:SSL with two-way authentication)
3) Import Client's Certificate to TrustStore for Object Operations
4) Import Client's Certificate to TrustStore for Event Indications
5) Export Server's Certificate from KeyStore for Object Operations
6) Export Server's Certificate from KeyStore for Event Indications
7) Exit
>
```

3. To disable two-way authentication for object operations, enter 1 in the SMI-S main panel. To disable two-way authentication for event indications, enter 2 in the SMI-S main panel.

A panel appears as in the example below.

```
You must stop the Device Manager Server before specifying this setting.
1) SSL without two-way authentication
2) SSL with two-way authentication
>
```

4. Stop the Device Manager server as indicated in the displayed message.

Stop the Device Manager server as follows:

- In Windows:
Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.
- In Solaris or Linux:
Execute the following command:
/opt/HiCommand/suitesrvctl -stop_hdvm

5. Enter 1.

The `mofcomp` command is executed and the MOF file is compiled.

You are returned to the SMI-S main panel when the `mofcomp` command has completed execution.

Caution: If you type the same number as the current setting, you are immediately returned to the SMI-S main panel.

Caution: If `mofcomp` command execution fails, the following message appears: The compilation of the MOF file failed. In this case, collect all files in the following directory and contact maintenance personnel.

- In Windows:

*nstallation-folder-for-the-Device-Manager-
Server\HiCommandServer\wsi\server\jserver\mof*

- In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/server/jserver/mof

6. Start the Device Manager Server.

Start the Device Manager server as follows:

- In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Start Server**.

- In Solaris or Linux:

Execute the following command:

/opt/HiCommand/suitesrvctl -start_hdvm

7.5 Authenticating File Operations Using a Java Tool

This section describes the following operations required for SSL-encrypted communication between the Device Manager server and the CIM client using CIM/WBEM functionality:

- Creating a keystore file
- Exporting authentication files from a keystore file
- Creating a truststore file and importing authentication files

These operations use the Java `keytool` command (equivalent to JDK1.4.0). The `keytool` command is installed in the following location when Device Manager is installed:

In Windows:

```
installation-folder-for-HiCommand-Suite-Common-  
Component\jdk\bin\keytool.exe
```

In Solaris or Linux:

```
/opt/HiCommand/Base/jdk/bin/keytool
```

In the `keytool` command, specify the file name, alias, and password for the keystore file or the truststore file. Note the following when specifying these items:

- Do not use the following symbols in the file name:
: , ; * ? " < > |
- Specify the file name as a character string of no more than 255 bytes.
- Do not include double quotation marks (") in the alias or password.

Note: This section assumes that a path to the `keytool` command has been added to the environment variable `PATH`.

7.5.1 Creating a Keystore File

To create a keystore file:

1. Execute the following command:

```
keytool -genkey -keystore keystore-filename -storepass keystore-password -alias alias -  
dname entity-distinguished-name -validity validity-of-certificate -keypass keypass -  
keyalg RSA
```

Note: Specify the same password for `-storepass` and `-keypass`.

Example of executing the command:

```
> keytool -genkey -keystore .keystore -storepass sanssl -alias san3gssl -dname  
"CN=san3g, OU=SSL, O=hitachi, L=yokohama, S=kanagawa, C=JP" -validity 720 -keypass  
sanssl -keyalg RSA
```

2. Check the created keystore file.

Execute the following command:

```
keytool -list -keystore keystore-filename -storepass keystore-  
password
```


7.5.2 Exporting an Authentication File from a Keystore File

To export an authentication file from a keystore file:

1. Execute the following command:

```
keytool -export -keystore keystore-filename -storepass keystore-password -alias alias  
-file authentication-file-name
```

2. Check the exported authentication file using the following command:

```
keytool -printcert -v -file authentication-file-name
```

7.5.3 Creating a Truststore File and Importing an Authentication File

To create a truststore file and import the authentication file:

1. Execute the following command:

```
keytool -import -alias alias -keystore truststore-filename -storepass truststore-  
password -trustcacerts -file authentication-filename
```

2. Check the created keystore file:

```
keytool -list -keystore truststore-filename -storepass truststore-password
```


Chapter 8 HiCommand Device Manager Server Properties

- Overview of HiCommand Device Manager Server Properties (see section 8.1)
- Server Configuration Properties (see section 8.2)
- Database Properties (see section 8.3)
- Logger Properties (see section 8.4)
- Dispatcher Properties (see section 8.5)
- MIME Properties (see section 8.6)
- Client Properties (see section 8.7)
- Security Properties (see section 8.8)
- SNMP Trap Properties (see section 8.9)
- Launchable Applications Properties (see section 8.10)
- Mainframe Host Agent Properties (see section 8.11)
- Restrictions on Web Clients Connected to the Device Manager Server (see section 8.12)

8.1 Overview of HiCommand Device Manager Server Properties

In Windows systems, the default directory for the configuration definition file is:

```
c:\Program Files\DeviceManager\HiCommandServer\config
```

In Solaris or Linux systems, the default directory for the configuration definition file is:

```
/opt/HiCommand/HiCommandServer/config
```

Important: If you make a change to any property file, that change will not take effect until the server is rebooted. If you make changes to any server properties, you will need to restart the Device Manager Agent.

- Server properties include web configuration properties and performance properties (see section 8.2). Web configuration properties include the IP address and port of the HTTP listener(s), the location of the server's document directory, and the name of the default index page. Performance properties include the size of input/output buffers, various TCP/IP stack and socket settings, server file-cache parameters, and connection thread priorities.

WARNING: You should not undertake the task of optimizing these attributes unless you are an expert, because even minor changes could severely impact the performance of the Device Manager Server.

- Database properties (see section 8.3) include DBMS parameters, such as drivers and logon ID.

WARNING: You should not undertake the task of optimizing these attributes unless you are an expert, since minor changes could severely impact the performance of the Device Manager Server.

- Logger properties (see section 8.3.2) include directives that configure Device Manager Server's logging module, including the names, locations and verbosity level of operational and error logging of the various log files.
- Dispatcher properties (see section 8.5) include properties that allow the fine-tuning of various background processes (daemons) and the optimization of the thread-priority for service agents.
- MIME properties (see section 8.6) include the translation/lookup table for all Multipurpose Internet Mail Extensions (MIME) file types recognized by the Device Manager Server.
- Client properties (see section 8.7) include properties that configure the Device Manager Web Client.
- Server security properties (see section 8.8) include whether secure-socket encryption is being utilized, the location and passwords for the Server Certificate TrustStore, a list of permitted client IP addresses, and properties that support the hardening of the Device Manager Server against certain kinds of denial-of-service attacks.
- SNMP trap properties (see section 8.9) include whether to enable Device Manager to use the SNMP trap function and whether to customize the trap list.
- Launchable application properties (see section 8.10) include the necessary information for launching related applications.
- Mainframe Host Agent Properties (see section 8.11) include the settings for communication between the Device Manager server and mainframe hosts.

These files are in Java™ property file format, and except for the security properties file can be modified using any text editor. Each property directive consists of a name-value pair separated by the equal sign (for example, `foo.bar=12345`). The appropriate end-of-line terminator, as defined by the operating system, delineates individual properties.

Comments in Device Manager property files are tagged using the `"#"` character at the start of a line. Literals (text strings or numeric values) do not need to be quoted. Boolean values can be either true or false (case-insensitive). Any other setting (for example, yes) is interpreted as false.

The backslash is a reserved character in Java property files, and is used for escaping various control characters such as tabs, line-feeds, etc. On Windows platforms absolute pathnames typically contain backslash characters, and must be backslash-escaped, for example, the file pathname `c:\HiCommand\docroot\foo.bar` should be entered as `c:\\HiCommand\\docroot\\foo.bar`. There is generally no need to backslash-escape any other characters in the property directives.

WARNING: As a general rule, server properties should not need to be modified. Use extreme caution when you are modifying the configuration properties, because you can cause the server to fail or to function incorrectly. Do not modify server properties unless you have sufficient expertise to understand the potential consequences of your actions.

Table 8.1 summarizes the various Device Manager property files.

Table 8.1 Summary of Device Manager Property Files

Property	Description	Location
Server Configuration Properties	These files relate to server performance properties, including the size of input/output buffers, various TCP/IP stack and socket settings, server file-cache parameters, and connection thread priorities.	Section 8.2
server.http.host	Designates either the host name or the dotted-decimal IP address for the Device Manager web server.	Section 8.2.1
server.http.port	Assigns the port used for the Device Manager HTTP server.	Section 8.2.2
server.https.port	Assigns the port used for the Device Manager secure HTTP server.	Section 8.2.3
server.http.default	Sets the name of the default index page for the Device Manager web server.	Section 8.2.4
server.http.request.timeout	Sets the read-blocking timeout of the HTTP socket connection.	Section 8.2.5
server.http.connection.priority	Sets the priority for all client-connection threads spawned by HTTP requests made against the Device Manager Server.	Section 8.2.6
server.http.connection.bufSize	Sets the size (in bytes) for the server's input/output (I/O) buffers.	Section 8.2.7
server.http.socket.backlog	Assigns the maximum queue length for incoming connection indications.	Section 8.2.8
server.http.socket.maxThreads	Sets the maximum number of concurrent connections accepted by the Device Manager Server.	Section 8.2.9
server.http.socket.linger	Toggles whether the SO_LINGER socket attribute is enabled for client connections with the Device Manager Server.	Section 8.2.10
server.http.socket.noDelay	Toggles whether the TCP_NODELAY socket attribute is enabled for connections to the Device Manager Server.	Section 8.2.11
server.http.headers.maxNumber	Sets the maximum number of HTTP headers permitted for any request submitted to the Device Manager web server.	Section 8.2.12
server.http.headers.maxLength	Sets the maximum length permitted for any HTTP header.	Section 8.2.13
server.http.entity.maxLength	Sets the maximum length of an HTTP request entity.	Section 8.2.14
server.http.log.reverseDNS	Flags whether the Device Manager Server performs reverse-DNS (Domain Name Server) lookup for its access logging.	Section 8.2.15
server.http.cache.size	Sets the upper-limit size of the Device Manager Server's internal file cache.	Section 8.2.16
server.http.cache.maxFileSize	Sets the maximum file size for server-side caching.	Section 8.2.17
server.http.fileTypes.noLog	Contains a comma-delimited list of the file types that are not logged in the Device Manager Server's access log when being transferred via HTTP.	Section 8.2.18
server.http.mode	This property sets whether the server is running in real mode or simulation mode.	Section 8.2.19
server.installTime	This property contains the install date of Device Manager.	Section 8.2.20
server.base.home	This property contains the installation directory of the Common Component.	Section 8.2.21

server.horcmconfigfile.hostname	This property allows you to specify whether to use the host name (hostname) or the IP address (ipaddress) when Device Manager edits the configuration definition file.	Section 8.2.22
server.base.initialsynchro	This property allows you to specify whether to synchronize the management information database and the displayed information (HiCommand Suite Common Repository) when you start Device Manager.	Section 8.2.23
server.cim.support	Determines whether CIM support is enabled.	Section 8.2.24
server.cim.support.protocol	Specifies whether to open or close the ports used by the CIM function.	Section 8.2.25
server.cim.http.port	Specifies the port for non- SSL transmission, for the CIM function.	Section 8.2.26
server.cim.https.port	Specifies the port for CIM SSL transmission.	Section 8.2.27
server.configchange.enabled	Determines whether to enable the automatic refresh function.	Section 8.2.28
server.configchange.autorefresh.lastrefreshed	Specifies whether to update the time of the last refresh, during automatic refreshing.	section 8.2.29
Database Properties	These files contain the set of directives that pertain to establishing a connection with the Device Manager Server's database.	Section 8.3
dbm.traceSQL	Designates whether output SQL to trace.log or not	Section 8.3.1
dbm.startingCheck.retryCount	Specifies the number of times the Device Manager Server retries the checking whether DBMS has started.	Section 8.3.2
dbm.startingCheck.retryPeriod	Specifies the interval (in seconds) at which the Device Manager Server retries the checking whether DBMS has started.	Section 8.3.3
Logger Properties	These files contain a set of directives that configure Device Manager Server's logging module, including the names, locations and verbosity level of operational and error logging of the various log files.	Section 8.4
logger.loglevel	Determines the verbosity level of operational (trace) and error logging.	Section 8.4.1
logger.MaxBackupIndex	Sets the number of rolling backups to keep of each log file before the oldest is erased.	Section 8.4.2
logger.MaxFileSize	Allows you to specify the maximum size for each log file.	Section 8.4.3
logger.hicommandbase.loglevel	Determines the verbosity level of operational (trace) and error logging which writes into HDvMtrace1.log by the Common Component	Section 8.4.4
logger.hicommandbase.sysloglevel	This property determines the verbosity level of operational (trace) and error logging which writes into the EventLog (for Windows) or the syslog (In Solaris or Linux systems) by the Common Component.	Section 8.4.5
logger.hicommandbase.MaxBackupIndex	This property sets the number of rolling backups to keep of HDvMtrace1 log file before the oldest is deleted.	Section 8.4.6
logger.hicommandbase.MaxFileSize	This property sets the number of rolling backups to keep of HDvMtrace1 log file before the oldest is deleted.	Section 8.4.7
Dispatcher properties	These files contain a set of configurable directives pertaining to the operation of Device Manager Server's dispatcher layer, including properties that allow the fine-tuning of various background processes (daemons) and the	Section 8.5

	optimization of the thread-priority for service agents.	
server.dispatcher.agent.priority	Assigns the priority for Device Manager service agent threads.	Section 8.5.1
server.dispatcher.message.timeout	Sets the timeout for pending response messages before they are expired (purged).	Section 8.5.2
server.dispatcher.message.timeout.in.processing	Sets the timeout for processing messages (in minutes) that are not completed by some reason.	Section 8.5.3
server.dispatcher.daemon.pollingPeriod	Defines the polling interval for the background agents responsible for checking component status and configuration version.	Section 8.5.4
server.dispatcher.traps.purgePeriod	Defines the purging interval for stale SNMP traps or alerts.	Section 8.5.5
server.dispatcher.startTimeOfIgnoringConnectionAlert	Defines the start time of the interval for stopping SNMP communication alert.	Section 8.5.6
server.dispatcher.endTimeOfIgnoringConnectionAlert	Defines the end time of the interval for stopping SNMP communication alert.	Section 8.5.7
server.dispatcher.daemon.receiveTrap	Determines whether or not port 162 is used as an SNMP trap.	Section 8.5.8
MIME Properties	These files contain the translation/lookup table for all Multipurpose Internet Mail Extensions (MIME) file types recognized by the Device Manager web server.	Section 8.6
Client Properties	These files affect the configuration of Device Manager Web Client.	Section 8.7
client.logger.trace	Defines whether or not to output trace log information.	Section 8.7.1
client.message.timeout	Defines the maximum wait time for the Device Manager Server response (timeout of connection) in seconds.	Section 8.7.2
client.ouputhorcmfunction.enabled	Specifies whether to enable Web Client to use CCI to create a configuration definition file.	Section 8.7.3
table.ldev.rowsperpage	Specifies the values displayed in the drop-down list used for setting the number of lines displayed per page on a window using a Web Client sortable table.	Section 8.7.4
client.assignlun.upperlimit.enabled	Enables you to make the upper limit check enabled or disabled for the number of LUNs that are assigned when storage is added.	Section 8.7.5
Security Properties	These files include whether secure-socket encryption is being utilized, the location and passwords for the Server Certificate TrustStore, and a list of permitted client IP addresses. This group also contains a number of properties that support the hardening of the Device Manager Server. WARNING: Do not use a text editor to change these properties. See Chapter 7 for more information on modifying security properties.	Section 8.8
server.http.secure	Sets the security level of the Device Manager Server.	Section 8.8.1
server.http.security.realm	Sets the security realm message for the Device Manager Server's authentication challenge.	Section 8.8.2
server.http.security.clientIP	Implements an IP address filter.	Section 8.8.3
server.https.security.keystore	Assigns the name of the Keystore file that contains a Server Certificate used for establishing an encrypted communication via Secure Sockets Layer (SSL) and Transport Layer Security (TLS).	Section 8.8.4

server.https.keystore.passphrase	Contains the logon password for the Keystore file that contains a keypair and associated Server Certificate used for SSL/TLS connections.	Section 8.8.5
server.https.keystore.keypass	Contains the password for recovering the keypair and associated Server Certificate used for encrypting SSL/TLS connections from the Device Manager Server's Keystore.	Section 8.8.6
server.http.security.unprotected	Designates a comma-delimited list of any non-protected file resources under the server's document root.	Section 8.8.7
server.https.security.truststore	Assigns the name and location of the truststore file that contains the Server Certificates.	Section 8.8.8
server.https.truststore.passphrase	Contains the password used to access the default truststore distributed with the Java Runtime Environment.	Section 8.8.9
SNMP Trap log output function properties	These files include whether to allow Device Manager to use SNMP traps, and whether the trap list will be customized.	Section 8.9
customizedsnmptrap.customized SNMPTrapEnable	This property allows you to enable the SNMP trap log output function.	Section 8.9.2
customizedsnmptrap.customizelist	This property allows you to specify how to customize the SNMP trap log output.	Section 8.9.3
Link and Launch Properties	These properties include server information about applications that can be launched from the GUI.	Section 8.10
launchapp.damp.url	This property specifies a URL for accessing the DAMP installation directory from a client web browser.	Section 8.10.1
<i>Mainframe host agent properties</i>	These properties include settings for communication between the Device Manager server and mainframe hosts.	Section 8.11
host.mf.agent.connection.timeout	Specifies the timeout for communication processing with a host agent.	Section 8.11.1

8.2 Server Configuration Properties

The server configuration properties are contained in the `server.properties` file. This is normally located in the `HiCommandServer/config` directory, under the installation directory.

The default directory for the configuration properties on Windows systems is:

```
c:\Program Files\Device Manager\HiCommand\HiCommandServer\config
```

The default directory for the configuration properties on Solaris or Linux systems is:

```
/opt/HiCommand/HiCommandServer/config
```

8.2.1 server.http.host

This property specifies either the host name or dotted-decimal IP address for the host that operates the web server functionality of Device Manager:

- If you specify a host name, make sure to use a value that a DNS can resolve on the Web Client, CLI, and the subsystem.

- If you specify an IP address, specify a value to which Web Client, CLI, and the subsystem can connect.
- In a cluster environment, specify the IP address of the cluster manager.
- When multiple NICs (Network Interface Cards) are installed on the server, specify a host name or IP address corresponding to an NIC to which Web Client, CLI, and the subsystem can connect.

Default: localhost

8.2.2 server.http.port

This property assigns the port used for the Device Manager HTTP (web) server. The conventional port number used for a standard web server is 80, but there may already be an Intranet server running on this port. Moreover, you should avoid low-numbered ports because these could conflict with other services installed on the server. As a general rule, you can pick any port between 1024 and 49151.

Caution: Use 80 for the port number when this property is set to a space character.

Default: 2001

8.2.3 server.https.port

This property assigns the port used for the Device Manager secure HTTP web server. The conventional port number for a secure web server is 443, but there may already be a secure Intranet server running on this port. As noted above, it is better practice to utilize a port number between 1024 and 49151 for a specialized (middleware) HTTP server. Make sure that it has a different value than the port designated for the HTTP listener.

Default: 2443

8.2.4 server.http.default

This property sets the name of the default index page for the Device Manager web server. If an HTTP request is made against a directory (for example, `https://hic.domain.com:2443/foo/`, where `foo` is a folder under the server's document root), the web server attempts to find and transfer the named file to the client. If none exists, a directory listing is returned to the client browser. Under normal conditions, you should not need to change the default value of this property.

Default: index.html

8.2.5 `server.http.request.timeout`

This property sets the read-blocking timeout of the HTTP socket connection (in milliseconds). It can be used to enable or disable the `SO_TIMEOUT` setting for client-connection sockets. Reading from the input stream associated with a socket will block for only this amount of time before the socket expires. Its default value is 5000 (5 seconds). A value of zero is interpreted as an infinite timeout, meaning that `SO_TIMEOUT` is disabled for client connections. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: 5000 (5 seconds)

8.2.6 `server.http.connection.priority`

This property sets the priority for all client-connection threads spawned by HTTP requests made against the Device Manager Server. Valid values are between 1 and 10 (1 = minimum priority; 5 = normal priority; 10 = maximum priority). You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance. Recommended values are between 5 and 8.

Note: If the connection thread priority is set to 10 (maximum), any simultaneous request connections are queued for sequential processing, which defeats the purpose of a multi-threaded server. This setting would actually adversely affect server performance, particularly when you are loading complex HTML pages (for example, those containing many images).

Default: 7

8.2.7 `server.http.connection.bufSize`

This property sets the size (in bytes) for all of the server's input/output (I/O) buffers. Increased buffer size may improve request/response network performance for high-volume connections, while decreasing it can help reduce the backlog of incoming data. Do not set the default value smaller than 1024 bytes, or it can cause failure. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: 8192 bytes

8.2.8 `server.http.socket.backlog`

This property assigns the maximum queue length for incoming connection indications (a request to connect), such as setting the `SO_MAX_CONN` attribute of the server socket. If a connection indication arrives when the queue is already full, the Device Manager Server will refuse the new connection. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: 50

8.2.9 `server.http.socket.maxThreads`

When a request has been issued and is being processed on the Device Manager Server, a client has an active connection on the server. This property specifies the number of active requests that can be processed at one time on Device Manager Server, not the maximum number of clients. Once this limit is reached, the next request will be dropped. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: 50

8.2.10 `server.http.socket.linger`

This Boolean property toggles whether the `SO_LINGER` socket attribute is enabled for client connections with the Device Manager Server. Setting this flag to its default value means a linger-On-close timeout of 60 seconds is applied to socket connections. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: true

8.2.11 `server.http.socket.noDelay`

This Boolean property toggles whether the `TCP_NODELAY` socket attribute is enabled for connections to the Device Manager Server. Setting this flag at its default value disables the Nagle algorithm for TCP/IP packets. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: true

8.2.12 `server.http.headers.maxNumber`

This property sets the maximum number of HTTP headers permitted for any request submitted to the Device Manager web server, and helps prevent certain types of denial of service and attempted buffer overflow attacks by restricting the effect of malicious requests containing a large number of headers. You should not need to change this setting under normal circumstances. The Device Manager Server silently ignores any HTTP headers in excess of this number. Runtime errors are not automatically generated under such circumstances.

Default: 20

8.2.13 server.http.headers.maxLength

This property sets the maximum length permitted for any HTTP header (in bytes). You should not need to change this setting under normal circumstances. It helps prevent certain types of denial of service and attempted buffer-overflow attacks by restricting the effect of malicious requests that contain unusually large header fields. Headers longer than the specified length will be truncated by the Device Manager Server without automatically generating runtime errors.

Default: 1024

8.2.14 server.http.entity.maxLength

This property sets the maximum length of an HTTP request entity (in bytes). You should not need to change this setting under normal circumstances. It helps prevent certain types of denial of service and attempted buffer overflow attacks by restricting the effect of malicious requests that contain unusually large payload entities. If the server detects a posted request longer than this value, it sends an error response to the client and logs details of the attempted request.

Default: 131072

8.2.15 server.http.log.reverseDNS

This Boolean property flags whether the Device Manager Server performs reverse-DNS (Domain Name Server) lookup for its access logging. When set, this property the server attempts to resolve the name of a client from the IP address for incoming connections. If the client's IP address can be resolved, the domain name is also written into the server's access log (for example, `http://www.hds.com/193.36.36.6`). Not all IP addresses on the Internet have an assigned domain name, so some logged requests might still be recorded as a numeric IP address, even with this flag turned on.

Note: While translation of the IP address to a domain name can assist analysis of the server's access logs, reverse-DNS lookups are expensive in terms of resources, and this feature may significantly degrade the server's performance, especially on a slow network. You should keep the setting at the default value for better performance.

Default: false

8.2.16 server.http.cache.size

This property sets the upper-limit size of the Device Manager Server's internal file cache (in bytes). A value of zero turns file caching off, which may adversely affect server performance when delivering complex static files (HTML pages containing images, etc).

This setting could be increased on a host machine with sufficient RAM installed. However, since the number of static files being served by Device Manager is only in the order of a few pages, performance gains would most likely be quite trivial.

Default: 10000000 bytes

8.2.17 server.http.cache.maxFileSize

This property sets the maximum file size for server-side caching. Static files larger than this limit (for example, the GUI application JAR file) are read from disk instead of being cached. There is no significant difference in response time whether these files are cached in memory or read directly from disk. A zero value for this property turns file caching off, which may adversely affect the web server's performance.

Default: 100000 bytes

8.2.18 server.http.fileTypes.noLog

This property contains a comma-delimited list of the file types that are not logged in the Device Manager Server's access log when being transferred via HTTP. Generally, logging should be performed only for the HTML pages being requested by a browser or other client, or the server's access log quickly becomes filled with entries for files such as graphics files, JavaScript™, or cascading style sheets.

The default value for this property eliminates logging for the majority of the resource-type files likely to be requested from the Device Manager web server. White space in the list is ignored. If you want access logging for all files, set this property to empty.

Default: gif,jpg,jpeg,png,css,js

8.2.19 server.http.mode

This property sets whether the server is running in real mode or simulation mode. This property is only used for development of the application that is connected to Device Manager. You should not change this property for normal operation.

Default: real

8.2.20 server.installTime

This property contains the Device Manager installation date.

Format: dd/mm/yyyy:HH:MM:SS ZZZZ (dd:day, mm:month, yyyy:year, HH:hour, MM:minute, SS:second ZZZZ (TimeZone)).

Default: dd/mm/yyyy:HH:MM:SS ZZZZ (Install date).

8.2.21 server.base.home

This property contains the installation directory of the Common Component, which is set by the Device Manager installer. You should not change this property under normal circumstances.

Default: (Value set by the installer)

8.2.22 server.horcmconfigfile.hostname

This property allows you to specify whether to use the host name (hostname) or the IP address (ipaddress) when Device Manager edits the configuration definition file.

Caution: Deleting a host name or an IP address that was specified when a copy pair was created disables operations on the copy pair. In such a case, refresh the subsystem information.

Default: ipaddress

8.2.23 server.base.initialsynchro

This property allows you to specify whether to synchronize the management information database and the displayed information (HiCommand Suite Common Repository) when you start Device Manager. A setting of true will synchronize the information. A setting of false will not synchronize the information.

Caution: If this property is set to **true**, synchronization of the information will take several minutes. If you change the property and then log in to Device Manager right away, an error may occur. If that occurs, wait until the synchronization is finished, and then log in.

Default: false

8.2.24 server.cim.support

This property determines whether CIM support is enabled. If you want to use a VDS service provider or execute CIM, you must set this property to **true**.

The installer sets this property to **true** if you enable the CIM/WBEM features for the SMI-S Provider service setting during installation (see Figure 3.5 or Figure 4.12).

Default: false

8.2.25 server.cim.support.protocol

This property sets whether to open or close the ports used by the CIM function. A value of 1 to 3 can be specified. When 1 is specified, the port for non-SSL transmission is opened and the port for SSL transmission is closed. When 2 is specified, the port for non-SSL transmission is closed and the port for SSL transmission is opened. When 3 is specified, both ports are opened.

If you decide not to use SSL when Device Manager is newly installed, 1 is set. If you select to use SSL, 3 is set.

Default: 3

8.2.26 server.cim.http.port

This property specifies the port for non-SSL transmission for the CIM function. If the SSL of the CIM function is disabled, `HITACHI_ObjectManager.Name` (a property of the CIM function) is set as this port.

For details on the `HITACHI_ObjectManager.Name` property, see the manual *HiCommand Device Manager CIM/WBEM User's Guide*.

Default: 5988

8.2.27 server.cim.https.port

This property specifies **HITACHI_ObjectManager.Name** as the port for the CIM function if SSL is enabled. For more information, see Hitachi Device Manager

Default: 5989

8.2.28 server.configchange.enabled

This property determines whether to enable the automatic refresh function. This function automatically performs a refresh when the Device Manager Server detects that the system configuration has been changed by the launched subsystem management tool (Storage Navigator or Storage Navigator Modular (for Web)). To enable this function, set this property to true.

Default: true

8.2.29 server.configchange.autorefresh.lastrefreshed

This property specifies whether the time of the last update is to be updated during an automatic refresh. (The time of the last refresh is always updated during a manual refresh, but this is an optional setting for an automatic refresh.) To specify that the time of the last update is to be updated during an automatic refresh, set this property to true.

Default: true

8.3 Database Properties

Database properties are contained in the database.properties file.

The database properties configuration file contains the set of directives that pertain to establishing a connection with the Device Manager Server's database. Before the Device Manager Server will run you need to correctly enter these settings and start the Database Management System (DBMS). If the server cannot connect to its DBMS, an entry is written to the error log (the default location is in the logs directory). This information can help considerably when you are troubleshooting a new installation.

This file also holds debugging and optimization property settings for the Java Database Connectivity (JDBC) layer in Device Manager Server. You should only modify these properties if you need detailed diagnostic information or if you are an expert System Administrator seeking to fine-tune certain aspects of performance and/or memory utilization.

The default directory for the Windows database properties file is:

c:\Program Files\DeviceManager\HiCommandServer\config

The default directory for Solaris or Linux logger properties file is:

/opt/HiCommand/HiCommandServer/config

8.3.1 dbm.traceSQL

This property designates whether the output to trace.log is SQL. Set true to output to SQL. Set false not to output SQL.

Default: false

8.3.2 dbm.startingCheck.retryCount

This property specifies the number of times the Device Manager Server will retry whether DMBS has started when the server is launched. The specifiable value ranges from 0 to 100. As a general rule, you do not need to change this setting.

Default: 18

8.3.3 dbm.startingCheck.retryPeriod

This property specifies the interval (in seconds) the Device Manager Server will retry whether DMBS has started when the server is launched. The specifiable value ranges from 0 to 100. As a general rule, you do not need to change this setting.

Default: 10 seconds

8.4 Logger Properties

Logger properties are contained in the `logger.properties` file.

This properties file contains a set of directives that configure Device Manager Server's logging module, including the names, locations and verbosity level of operational and error logging of the various log files. You can also use this file to configure trace logging for debugging and diagnostic purposes. The applicable file names are `access.log`, `error.log`, `service.log`, and `trace.log`.

The default directory for the Windows logger properties file is:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

The Windows event log is located in the event viewer.

The default directory for Solaris or Linux logger properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

The default syslog is specified in `/etc/syslog.conf`

8.4.1 logger.loglevel

This property determines the verbosity level of operational (trace) and error logging. The values accepted in this field are (in decreasing order of detail): `DEBUG`, `INFO`, `WARN`, `ERROR`, and `FATAL`. The default logging level for production systems is `INFO`, which means that debugging or informational entries as well as warnings and error messages are written into the trace and error logs.

Default: `INFO`

8.4.2 logger.MaxBackupIndex

This property sets the number of rolling backups to keep of each log file before the oldest is deleted. If this property is set to zero, no rolling backups are created, and log files are simply truncated when their maximum file size is reached. When a log file reaches its maximum length its filename is modified by appending a counter, for example, `access.log.1`. As more backup log files are created, their counter or version suffix is incremented (for example, `access.log.1` becomes `access.log.2`), until the specified number of rolling backups have been created. After that, the oldest backup log file is deleted each time a new backup is created. You can specify a range of 1 to 20.

Default: `10`

8.4.3 logger.MaxFileSize

This property allows you to specify the maximum size for each log file. Unless `KB` is specified for kilobytes or `MB` for megabytes, bytes is assumed. In this property, the term `KB` is interpreted as 1024 bytes, and `MB` as 1024 kilobytes.

Specifiable range: from 512 KB to 32 MB

Default: 1 MB

8.4.4 `logger.hicommandbase.loglevel`

This property determines the verbosity level of operational (trace) and error logging which writes into HDvMtrace1.log by the Common Component. Each logging event has its own importance level independent from its type (error, warning, and information). The levels, in increasing order of importance, are: 30, 20, 10, and 0. The default logging level for production systems is 20, which means that messages for logging event levels 20, 10, and 0 are written into the HDvMtrace1.log, but messages for logging event level 30 are not.

Default: 20

8.4.5 `logger.hicommandbase.sysloglevel`

This property determines the verbosity level of operational (trace) and error logging which writes into the EventLog (Windows) or the syslog (Solaris or Linux) by the Common Component. Each logging event has its own importance level independent from its type (error, warning, and information). The levels, in increasing order of importance, are: 30, 20, 10 and 0. The default logging level for production systems is 0, which means that messages for only the logging event leveled 0 are written into the EventLog (Windows) or the syslog (Solaris or Linux), but messages for the logging event leveled 30, 20, and 10 are not. The default value is recommended.

Default: 0

8.4.6 `logger.hicommandbase.MaxBackupIndex`

This property sets the maximum number of files to keep of the HDvMtrace1 log file before the oldest is deleted. Valid values are between 1 and 16. When a log file reaches its maximum length, its filename is modified by increasing a counter (e.g., for example, HDvMtrace2). As more backup log files are created, their counter or version suffix is incremented (e.g., HDvMtrace2.log becomes HDvMtrace3.log), until the specified number of rolling backups have been created. After that, the oldest backup log file is deleted each time a new backup is created.

Default: 10

8.4.7 `logger.hicommandbase.MaxFileSize`

This property sets the maximum size of each of the rolling backup Device Manager trace log files. The specified size is assumed to be in bytes unless you specify kB for kilobytes, MB for megabytes or GB for gigabytes. Valid values are between 4096 and 2147483647. Even if this directive is not found in the properties file, an internal default value of 1 MB will be used.

Default: 1 MB

8.5 Dispatcher Properties

Dispatcher properties are contained in the `dispatcher.properties` file.

This properties file contains a set of configurable directives pertaining to the operation of Device Manager Server's dispatcher layer, including properties that allow the fine-tuning of various background processes (daemons) and the optimization of the thread-priority for service agents.

The default directory for the Windows dispatcher properties file is:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

The default directory for Solaris or Linux logger properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

8.5.1 `server.dispatcher.agent.priority`

This property assigns the priority for Device Manager Agent threads. Valid values are between 1 and 10 (1 = minimum priority; 5 = normal priority; 10 = maximum priority). You should change the default value only if you need to fine-tune the agent dispatcher's performance. The recommended values are between 5 and 8, and you should not set it to the maximum thread priority (9-10), because while that may cause individual requests to execute faster, it is likely to cause an overall degradation in performance when multiple users are sending concurrent requests.

Default: 5

8.5.2 `server.dispatcher.message.timeout`

This property sets the timeout for pending response messages (in minutes) before they are expired (purged). A pending message consists of a response from a long-running process (for example, discovery of a storage array) that has not yet been either polled by the client or sent to the client via the Device Manager notification service.

Default: 15 minutes

8.5.3 `server.dispatcher.message.timeout.in.processing`

This property sets the timeout for processing messages (in minutes) that are not completed by some reason.

Default: 720 minutes

8.5.4 server.dispatcher.daemon.pollingPeriod

This property defines the polling interval (in minutes) for the background agents responsible for checking component status and configuration version. A value of zero will disable these polling agents.

Default: 5 minutes

8.5.5 server.dispatcher.traps.purgePeriod

This property defines the purging interval for stale SNMP traps or alerts (in minutes). A value of zero will disable the purging of traps from the server.

Default: 5 minutes

8.5.6 server.dispatcher.startTimeOfIgnoringConnectionAlert

This property defines the start time of the interval for stopping SNMP communication alert. Accessing the subsystem that is in regular reboot will incur this alert.

Default: 2:45

8.5.7 server.dispatcher.endTimeOfIgnoringConnectionAlert

This property defines the end time of the interval for stopping SNMP communication alert. If you access a subsystem that is in regular reboot, that will cause this alert.

Default: 3:15

8.5.8 server.dispatcher.daemon.receiveTrap

This property determines whether or not port 162 is used as an SNMP Trap listener. Device Manager can use SNMP to detect command completion and hardware issues. If port 162 is in use, Device Manager can use polling to determine these issues, but using SNMP is preferred.

If the SNMP trap is set, then Device Manager Server is started and port 162 is in use, the server will output an error message and stop. During installation, the SNMP Trap Note panel is displayed to warn the user of this potential outcome.

The default value of this property is **true**, which enables the SNMP Trap reception function. If you set this property to **false**, the function is disabled. If you choose to disable the function during a new installation, the installer automatically sets this property to **false**.

Default: True

8.6 MIME Properties

MIME properties are contained in the mime.properties file.

This file contains the translation/lookup table for all Multipurpose Internet Mail Extensions (MIME) file types recognized by the Device Manager web server. Each property in this lookup table maps a particular extension suffix to the MIME type for that file. You should not need to modify this setting under normal circumstances, and in any event only expert System Administrators should make any additions to this file.

The default directory for the Windows MIME properties file is:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

The default directory for Solaris or Linux logger properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

8.7 Client Properties

Client properties are contained in the client.properties file. This properties file contains the configuration information for the Device Manager Web Client.

In Windows, the default directory for the client properties file is as follows:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris or Linux, the default directory for the client properties file is as follows:

```
/opt/HiCommand/HiCommandServer/config
```

8.7.1 client.logger.trace

This property defines whether output the trace information or not by applying Java Web Start's log output function. Set this property to true to output trace information. Set this property to false to not output trace information.

Note: In order to output trace information, Java Web Start's log output function must be activated. See *HiCommand Device Manager Web Client User's Guide* for more information about the Java Web Start log output function.

Default: false

8.7.2 client.message.timeout

This property defines the maximum wait time for the Device Manager Server response (timeout of connection) in seconds. Web Client sends the notification messages to the server, and the server sends the notification of the task complete or the alert in response. The connection between the client and the server is on while waiting the response of the notification from the server. This property sets the timeout of this waiting time. The client sends the notification message again after the timeout. This timeout will be applied each time Web Client accesses the server.

Note: When the client is accessing the server through a proxy server and the connection timeout of the proxy is shorter than the timeout of this property, the notification message may be lost, because the timeout of the proxy server cuts the connection before the Device Manager Server can send the response to the Web Client. If this is the case, please set the timeout for this property to a time shorter than the timeout of the proxy.

Default: 300 seconds

8.7.3 client.outputorcmfunction.enabled

This property enables Web Client to use CCI to create a configuration definition file. Set this property to true to enable the use of this function.

Default: false

8.7.4 table.ldev.rowsperpage

Specifies the values displayed in the drop-down list used for setting the number of lines displayed per page on a window using a Web Client sortable table. The values set by this property appear in a Web Client drop-down list. Up to two choices for the number of lines can be included in the drop-down list. To set two choices, specify the two values separated by a comma. The minimum number of lines that can be specified is 1. The maximum number of lines that can be specified depends on the environment, such as the Web browser the client uses and the CPU performance and memory capacity of the client machine. The maximum number of lines (standard) for each Web browser is as follows:

- Internet Explorer 6.0: 1000
- Mozilla 1.4: 2000
- Mozilla 1.7: 300

If you specify a value larger than the maximum value (standard), a warning dialog box may appear indicating that the machine may be unable to respond. If this occurs, decrease the value of the property and restart HiCommand Suite Common Component.

8.7.5 client.assignlun.upperlimit.enabled

This property enables you to make the upper limit check enabled or disabled for the number of LUNs that are assigned when storage is added.

When *LUN assignment*, which is a step of the storage addition function, is performed in a state where many volume paths have already been determined, HBase Storage Mgmt Common Service might stop running. This problem occurs when the size of the memory required to keep the display information for *LUN assignment* and the log output information exceeds the upper limit of the JAVA heap size for HBase Storage Mgmt Common Service. Therefore, to prevent HBase Storage Mgmt Common Service from stopping, set and check the upper limit for the number of LUNs that can be assigned in a single operation. The upper limit of the number of LUNs, which is used for the check, is 100. To enable the check, specify `true`, and to disable the check, specify `false`.

Default: `true`

8.8 Security Properties

Server security properties are contained in the `server.properties` and `security.properties` files. These files include whether secure-socket encryption is being utilized, the location and passwords for the Server Certificate TrustStore, and a list of permitted client IP addresses. This group also contains a number of properties that support the hardening of the Device Manager Server.

In Windows or Linux, the default directory for the security properties file is as follows:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris, the default directory for the security properties file is as follows:

```
/opt/HiCommand/HiCommandServer/config
```

WARNING: Do not use a text editor to edit these properties. See Chapter 7 for more information on changing security properties.

8.8.1 server.http.secure

This property sets the security level of the Device Manager Server. See section 7.2.2 for instructions on how to use HiKeytool to set the security level, as follows:

- 0 = Unsecure. Any client application can obtain access to the server. No logon authentication is required from the client. This setting is intended for use only on highly secure LANs and/or private networks, and even in those environments more robust server security is highly recommended.
- 1 = Basic Authentication. The Device Manager Server is operating in protected mode, and client applications attempting to connect with the server must submit an authorized user's logon ID and password and be authenticated against the Access Control List (ACL).

Note: These requirements do not apply to requests for files that are intentionally designated as being excluded from ACL security protection (see the `server.http.security.unprotected` property in section 8.8.7).

- 2 = Secure Socket (TLS/SSL). In this security mode, the server opens an additional secure HTTP listener on a port designated by the `server.https.port` property. All communications via this port are strongly encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). Refer to Chapter 7 for further information on SSL and TLS. In order for a server to use the secure HTTP protocol, a keypair and associated Server Certificate must be present in the Device Manager Server Keystore. This setting is strongly recommended if a Device Manager Server is exposed to any public network or Internet.

Default: 1

8.8.2 `server.http.security.realm`

This property sets the security realm message for the Device Manager Server's authentication challenge. This text is usually displayed in a browser's logon dialog.

Default: `Device Manager Security`

8.8.3 `server.http.security.clientIP`

This property implements an IP address filter, which helps harden a server against malicious attacks. The default value is `*.*.*` which means that an HTTP connection from any client IP address will be accepted. You can restrict the Device Manager Server access to designated clients and/or to subnets such as a Local Area Network (LAN) or Wide Area Network (WAN), by using asterisks as a wildcard character. For example, a Device Manager Server would only accept connections from the host machine itself and other client users on a LAN if this directive was set as:

`server.http.security.clientIP=127.0.0.1,192.168.*.*`

White space (the space following the comma delimiter) is ignored, as are any invalid dotted-decimal IP entries, so that no runtime error is raised if an invalid or incorrectly formatted network address is detected in this list.

Client machines that are not on the access list will be denied access to the server, however access from the Web Client cannot be restricted. No HTTP response message (stating a reason for the failure to establish a connection) will be returned to the intruder, in order to reduce vulnerability to certain denial of service attacks that attempt to overload a server by flooding it with a large number of simultaneous (bogus) requests.

Default: `*.*.*`

8.8.4 `server.https.security.keystore`

This property assigns the name of the Keystore file that contains the keypair and associated Server Certificate used for establishing an encrypted communication via Secure Sockets Layer(SSL) or Transport Layer Security. The default setting is `Keystore`, and this file is assumed to be located in the Device Manager Server's installation directory.

The Keystore file shipped with a Device Manager Server is an empty placeholder file that does not contain the required keypair and associated Server Certificate needed to run the Device Manager Server in secure mode. If you attempt to start the server in secure mode with an empty Keystore file, the server will log a fatal exception and fail. A keypair and associated self-signed or trusted certificate must first be installed into the Keystore before encrypted communications can be started. see section 7.2.3 for more information about Server Certificates.

Default: `keystore`

8.8.5 server.https.keystore.passphrase

This property contains the logon password for the Keystore file that contains a keypair and associated Server Certificate used for SSL/TLS connections. The logon password is used to check the integrity of the Keystore data. See section 7.2.6 for instructions on using HiKeytool to change the password.

Default: passphrase

8.8.6 server.https.keystore.keypass

This file contains the password for recovering the keypair and associated Server Certificate used for encrypting SSL/TLS connections from the Device Manager Server's Keystore (refer also to the server.https.security.keystore property in section 8.8.4). See section 7.2.7 for instructions on how to use HiKeytool to change the Keystore password.

Default: passphrase

8.8.7 server.http.security.unprotected

This property designates a comma-delimited list of any non-protected file resources under the server's document root. When files or directories are designated as unprotected, they are not subject to Access Control List checks (user authentication), regardless of the security mode setting for the server. Entire directories (including nested sub-directories) can be flagged as unprotected by using an asterisk as a wildcard character. If this directive is empty all resources are protected, so that every request to the Device Manager Server will require user authentication.

This property allows anyone to view the index.html front page via a browser, without user authentication being required. More importantly, it allows the Java Web Start application to update its JAR file and deploy (via the HiCommand.jnlp file) to the end-user's system without raising a series of logon dialogs. Similarly, the GUI's help files (and certain client installation information) can be viewed via a web browser without separate authentication being required at each step. The default should not require modification under normal circumstances.

Default: index.html, HiCommand/*, webstart/*, images/*, style/*, docs/*, favicon/ico

8.8.8 server.https.security.truststore

This property assigns the name and location of the truststore file that contains the Server Certificates. The Device Manager Server uses the default truststore distributed with the JRE named "cacerts".

Note: This property cannot be modified with HiKeytool. If you want to change the value, you must do so by editing the value in the server.properties file.

Default: `{java.home}/lib/security/cacerts`

8.8.9 server.https.truststore.passphrase

This property contains the password used to access the default truststore distributed with the Java Runtime Environment. For instructions on how to use HiKeytool to change the truststore password, see section 7.2.10.

Default: `changeit`.

8.9 SNMP Trap Properties

SNMP trap properties are contained in the customizedsnmptrap.properties file.

In Windows, the default directory for the SNMP trap properties file is:

```
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris or Linux, the default directory for the SNMP trap properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

Device Manager can be configured to output the SNMP Traps as a log file, which allows you to centrally monitor devices within a storage area and applications.

In Windows, the default directory for the SNMP trap properties file is as follows:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris or Linux, the default directory for the SNMP trap properties file is as follows:

```
/opt/HiCommand/HiCommandServer/config
```

The SNMP trap log has the following features:

- A log message contains information about the events related to a trap and the information that can identify where those events occurred.
- The trap to be logged is not limited to the trap related to storage devices. The traps related to the desired devices and applications can be output to logs uniformly.

- Each element of the acquired SNMP Trap is output to the log output message. The items to be output and their order can be customized.

The scope of the log output is as follows:

- Notification of an error or command completion (USP, 9900V, and 9900 only)
- Other SNMP traps (USP, 9900V, and 9900 only)
- SNMP traps for other devices (SNMP version 1 trap only)

The log message outputs the following information:

- Message ID indicating that a trap was received
- Sender (agent)
- Enterprise ID (enterprise)
- Generic trap number (generic)
- Specific trap number (specific)

Log messages are output to the following destinations:

- The output destinations for HiCommand Suite Common Component log messages (for details, see section 5.4):
 - Device Manager trace log file
 - HiCommand Suite common trace log file
 - Event log / syslog file
- The output destinations for log messages related to system startup processes:
 - Trace log file
 - Error log file[#]
- [#] This file is output only when the severity is Error, Critical, or Alert. For details on the severity, see Table 8.2.

8.9.1 Log output customization

By setting the `customizedsnmptrap.customizedSNMPTrapEnable` property to true, the SNMP Trap information can be output to log messages. You can customize the output information in the `customizedsnmptrap.customizelist` property. A customization definition for output log consists of five items separated by colons. You can omit some items, but may not omit the colon delimiter. To specify more than one customization definition, use a comma as a delimiter, but make sure not to enter a comma at the end of the last entry. To change the line in the middle of a customization list, enter a back slash (\) at the end of that line. The line feed following the back slash (\) is ignored.

The following shows the definition for log customization:

```
customizedsnmptrap.customizelist = \
enterprise-ID-1:generic-trap-number-1:specific-trap-number-1:severity-1:message-1, \
```

```
enterprise-ID-2:generic-trap-number-2:specific-trap-number-2:severity-2:message-2, \
...
enterprise-ID-n:generic-trap-number-n:specific-trap-number-n:severity-n:message-n
```

The following table lists and describes the format of each item used during customization definition.

Table 8.2 Format of Each Item Used for Customization Definition

Item	Format	Remarks
Enterprise ID	Specify by using a dot (e.g., .1.3.6.1.4.116.3.11.1.2)	Required
Generic trap number	Numeric value, from 0 to 6	Required
Specific trap number	Numeric value	Required
Severity	Information: -I WARNING: -W Error: -E Critical: -E Alert: -E Null: no output	Not required. When this is omitted, Null is used.
Message	Use the following character strings (variable) to specify message information to be output: \$a Agent address (dotted format) \$e Enterprise ID (dotted format) \$g Generic trap number \$s Specific trap number \$n (where n indicates an integer, which is 1 or larger): The value of the nth variable is binding	Not required. When this is omitted, \$a\$e\$g\$s is used.

The following shows an example of a customized log configuration:

```
customizedsnmptrap.customizelist = \
.1.2.3:6:1:Information:$a$e$g$s$1$2, \
.1.3.6.1.4.1.2854:6:1:Warning:$e$a$s$3$2$1$g, \
.1.3.6.1.4.1.116.3.11.4.1.1:6:1:ERROR:$a$s, \
.1.3.6.1.4.1.116.3.11.4.1.1:6:100:Information:$a$s
```

Figure 8.1 Sample Log Customization (1)

8.9.2 customizedsnmptrap.customizedSNMPTrapEnable

This property allows you to enable the SNMP trap log output function. Specify true to use the log output function, or false to not to use the function.

Default: false

8.9.3 customizedsnmptrap.customizelist

This property allows you to specify how to customize the SNMP trap log output. See section 8.9.1 for details.

Default: None

8.10 Launchable Applications Properties

This file contains information on launchable applications.

This properties file contains information for the server that contains the applications that can be launched.

In Windows, the default directory for the launchable application properties file is as follows:

c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config

In Solaris, the default directory for the launchable application properties file is as follows:

/opt/HiCommand/HiCommandServer/config

8.10.1 Launchapp.damp.url

This property specifies the URL of the web server for Storage Navigator Modular (for Web) or Damp (for Web) to be launched from the Web browser in a client.

Note: Even if this was previously set in the previous version, you must re-set it. If you change the value, restart the server and then refresh the subsystems.

The following shows an example of specifying the URL of the web server for Storage Navigator Modular (for Web):

launchapp.damp.url=http://192.168.17.235:23015/program/DeviceManager/snm

Important: Setting up alias information is necessary in order to use Storage Navigator Modular (for Web). For details on setting the environment information in one operation, see section 9.1.2.

The following shows an example of specifying the URL of the web server for DAMP (for Web):

launchapp.damp.url=http://192.168.17.235:23015/program/DeviceManager/damp

Important: Setting up alias information is necessary in order to use DAMP (for Web). For details on setting the environment information in one operation, see section 9.2.2

Default: Not applicable

8.10.2 launchapp.snm.rmi.port

When you have changed the port number used for RMI communication in Storage Navigator Modular (for Web), you need to specify the new port number in this property. If you do not do this, Device Manager cannot link with Storage Navigator Modular (for Web). Valid values are from 1 to 65535.

If you have not changed the port number used for communication, do not specify this property. For details on how to view and change the port number used for communication that is specified in Storage Navigator Modular (for Web), see the *Storage Navigator Modular (for Web) User's Guide*.

Default: None

8.11 Mainframe Host Agent Properties

Properties of the mainframe host agent are contained in the `host.properties` file.

This properties file contains settings for communication between the Device Manager server and mainframe hosts.

In Windows, the default directory for the mainframe host agent properties file is:

```
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris or Linux, the default directory for the mainframe host agent properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

8.11.1 host.mf.agent.connection.timeout

This property specifies the timeout (in seconds) for communication processing between the Device Manager server and a mainframe host agent. Valid values are 0 and from 30 to 3600. If you specify 0, no timeout applies. You should only modify this property if you are an expert System Administrator seeking to fine-tune performance of the mainframe host agent.

Default: 300

8.12 Restrictions on Web Clients Connected to the Device Manager Server

If the version of the Device Manager server is version 3.0 or later, restrict Web Clients that can connect to the Device Manager server by performing the following procedure. If the version is earlier than 3.0, perform only step 4 to restrict the Web Clients.

To restrict Web Clients that can connect to the Device Manager server:

1. Stop the Device Manager server and HiCommand Suite Common Component.
 - For Windows, select **Start, Program, HiCommand, Device Manager**, and then **Stop Server with Common Services**.
 - For Solaris or Linux, execute the following command:
/opt/HiCommand/suitesrvctl -stop_all
2. Open the `httpsd.conf` file, located in the following directory:
 - For Windows:

```
Installation-folder-for-HiCommand-Suite-Common-  
Component\httpsd\conf\httpsd.conf
```

– For Solaris or Linux:

```
/opt/HiCommand/Base/httpsd/conf/httpsd.conf
```

3. Register hosts that can be connected to the Device Manager Server in the last line of the `httpsd.conf` file.

The following shows the format for registering hosts in the `httpsd.conf` file:

```
<Location /DeviceManager>  
    order allow,deny  
    allow from host [host....]  
</Location>
```

Figure 8.2 Format for Registering Hosts in the `httpsd.conf` File

Hosts can be written in the following formats:

- The domain name (**example:** `hitachi.datasystem.com`)
- Part of the domain name (**example:** `hitachi`)
- The whole IP address (**example:** `10.1.2.3 127.0.0.1`)
- Part of the IP address (**example:** `10.1` which, in this case, means `10.1.0.0/16`)
- Network/Netmask format (dot notation) (**example:** `10.1.0.0/255.255.0.0`)
- Network/*n* (CIDR notation: *n* is the number of bits for identifying a network) (**example:** `10.1.0.0/16`)

If you want to specify two or more hosts in a command line for `allow from`, delimit the hosts with a space.

Multiple lines can be used to specify hosts for `allow from`.

If you attempt to connect from a machine which has Device Manager installed, you must also specify the local loop-back address (`127.0.0.1` or `localhost`).

Be sure to specify `order` in accordance with the specified format. If extra spaces or tabs are inserted, the operation will fail.

The following shows an example of registering hosts in the `httpsd.conf` file:

```
<Location /DeviceManager>  
    order allow,deny  
    allow from 127.0.0.1 10.0.0.1  
    allow from 10.0.0.0/26  
</Location>
```

Figure 8.3 Example of Registering Hosts to the `httpsd.conf` File

1. Register hosts to the `server.http.security.clientIP` property. For details on how to set the `server.http.security.clientIP` property, see section 3.3.4.
2. Restart the Device Manager Server and the HiCommand Suite Common Component.

- For Windows, execute the following command: Select **Start, Program, HiCommand, Device Manager**, and then **Start Server with Common Services**.
- For Solaris or Linux, execute the following command:

```
# /opt/HiCommand/Base/bin/hcmdssrv -start_all
```

3. Restart the Device Manager server.

- For Windows, select **Start-Programs-HiCommand-Device Manager-Start Server**.
- For Solaris, execute the following command:

```
# /opt/HiCommand/hicommand.sh start
```

Caution: If you log on to a HiCommand Suite product from a host that is not registered in the `httpsd.conf` file, the Device Manager server cannot be started from that HiCommand Suite product.

Chapter 9 Linking Device Manager With Other Products

This chapter describes the settings for linking Device Manager with related products.

- Linking With Storage Navigator Modular (for Web) (see section 9.1)
- Linking With DAMP (for Web) (see section 9.2)
- Starting HSSM From the Dashboard (see section 9.3)

9.1 Linking With Storage Navigator Modular (for Web)

This section describes prerequisites and environment setup for linking with Storage Navigator Modular (for Web).

Caution: The Linux version does not support linkage with Storage Navigator Modular (for Web).

9.1.1 Prerequisites for Using Storage Navigator Modular (for Web)

The prerequisites for using Storage Navigator Modular (for Web) are as follows:

- For details about the environment setup required for operating Storage Navigator Modular (for Web), see the *Storage Navigator Modular (for Web) User's Guide*.
- Install Storage Navigator Modular (for Web) on the machine where the Device Manager server is installed.
- To use Storage Navigator Modular (for Web), you must set up a Web server to run it.
- Use HiCommand Suite Common Component for the Web server that runs Storage Navigator Modular (for Web). HiCommand Suite Component is installed during installation of the HiCommand Device Manager server.
- Storage Navigator Modular (for Web) cannot be used together with DAMP (for Web).
- Multiple Storage Navigator Modular (for Web) clients cannot concurrently access the same storage subsystem.

Caution: The web server for Storage Navigator Modular (for Web) can be accessed via only one NIC even if multiple NICs are installed on the machine. To link with Storage Navigator Modular (for Web) in a machine environment where multiple NICs are installed, you need to specify the NIC to be used to access the web server for Storage Navigator Modular (for Web). The IP address or host name specified for this setting must be the same as that specified during installation of the Device Manager server. For details on how to specify the settings, see the *Storage Navigator Modular (for Web) User's Guide*.

Caution: To link with Storage Navigator Modular (for Web) in a cluster environment, the host you specify for accessing the Web server of Storage Navigator Modular must be identical to the logical host name you specified when installing the Device Manager server. For details on setting the host name, see the *Storage Navigator Modular (for Web) User's Guide*.

9.1.2 Setting the Launch Environment for Storage Navigator Modular (for Web)

Set the launch environment for Storage Navigator Modular (for Web) using the simple setup tool `launchapptool`.

The following conditions apply when setting the launch environment:

- The `launchapp.properties` file and `httpsd.conf` file must exist in the installation folder and must be write-enabled.
- HiRDB must be running.

Note: For details on the `launchapp.properties` file, see section 8.10.

Note: The `httpsd.conf` file is stored in the following location:

- In Windows:
`installation-folder-for-HiCommand-Suite-Common-Component\httpsd\conf`
- In Solaris:
`/opt/HiCommand/Base/httpsd/conf`

Note: For details on how to check the HiRDB operating status and start the HiRDB service, see section 5.3.1.

To specify the launch environment settings for Storage Navigator Modular (for Web):

1. Install Storage Navigator Modular (for Web).

For details on how to install Storage Navigator Modular (for Web), see the *Storage Navigator Modular (for Web) User's Guide*.

2. Execute the following command from the command prompt or terminal window:

- In Windows:
`installation-folder-for-the-Device-Manager-server\HiCommandServer\tools\launchapptool.bat`

The following shows an example of executing the command:

```
C:\Program
Files\HiCommand\DeviceManager\HiCommandServer\tools\launchapptool.bat
```

- In Solaris:
`# /opt/HiCommand/HiCommandServer/tools/launchapptool.sh`

3. The main menu appears. Select **1**.

```
=====
launchapptool
=====

1) Storage Navigator Modular (for Web) launch setup
2) Disk Array Management Program (for Web) launch setup
3) Delete launch settings
4) Exit

>1
```

Launch Settings for Storage Navigator Modular (for Web) will now Start.

4. If the launch environment settings for Storage Navigator Modular (for Web) have already been specified, a confirmation message asks if you want to change the current settings. Select **y** to change the settings, or **n** to leave the settings unchanged.

5. Specify the protocol to be used in the Web server URL. Select **1** to use http protocol, or **2** to use https protocol.

```
Specify the URL protocol.
1) http
2) https
   Caution: To use https, settings to enable SSL communication
             with the web server must be specified in advance.

Enter Value [default=1]
>1
```

Caution: For option **2**, the Web server must be set up for SSL communication.

6. Enter the IP address or host name to be used in the Web server's URL.

Specify an IP address or host name that can be accessed from the client machine on which the Web Client program is running.

```
Specify the IP address or hostname of the web server.
Enter Value [default=10.208.64.134]
>10.208.64.134
```

Note: To use a local host, specify its IP address rather than the host name.

7. Enter the port number to be used in the Web server's URL.

```
Specify the port number of the web server.
Enter Value [default=23015]
>23015
```

8. If you changed the port number for RMI communication in Storage Navigator Modular (for Web), enter the new port number.

```
Specify the port number for RMI communications.
Enter Value [default=1099]
>1099
```

Caution: Do not enter anything if you did not change the communication port number.

9. Enter the installation directory of Storage Navigator Modular (for Web).

```
Specify the installation directory path name of Storage Navigator Modular (for Web).
   Caution: Make sure that the specified installation directory
             path name ends with a forward slash (/).
   Caution: Replace backslashes (\) with forward slashes (/)
             in the specified installation directory path name.

Enter Value [default=C:/Program Files/Storage Navigator Modular Web/]
>D:/Storage Navigator Modular Web/
```

Caution: Make sure that the path ends with a forward slash (/).

Caution: In Windows, replace \ with / in the path name.

```
Example: "C:/Program Files/Storage Navigator Modular Web/"
```

10. Restart the Device Manager server and HiCommand Suite Common Component. For Windows, see section 3.5; for Solaris or Linux, see section 4.6.

The changes to the launch environment settings now apply.

```
Launch setup has successfully completed.
```

You must restart the Device Manager Server and Common Component Services for these changes to take effect.

Exit - Default is n?(y, n):

11. Check whether Storage Navigator Modular (for Web) runs on HiCommand Suite Common Component.

Specify the following URL in the browser, and then make sure that the Storage Navigator Modular (for Web) window appears.

`http://host-name-or-IP-address:portID/program/DeviceManager/snm/default.htm`

12. Refresh the storage subsystems to be operated on by Storage Navigator Modular (for Web).

Note: If you set up the launch environment by using the simple setup tool, the URL associated with Storage Navigator Modular (for Web) is set as alias information in HiCommand Suite Common Component. This alias information remains if you subsequently uninstall Device Manager or Storage Navigator Modular (for Web). To delete the alias information and other launch settings, see section 9.1.3.

Table 9.1 launchapptool Input Example (When Setting Storage Navigator Modular (for Web))

```
1) Storage Navigator Modular (for Web) launch setup
2) Disk Array Management Program (for Web) launch setup
3) Delete launch settings
4) Exit

>1

Launch Settings for Storage Navigator Modular (for Web) will now Start.

Specify the URL protocol.
1) http
2) https
   Caution: To use https, settings to enable SSL communication
              with the web server must be specified in advance.

Enter Value [default=1]
>1

Specify the IP address or hostname of the web server.
Enter Value [default=10.208.64.134]
>10.208.64.134

Specify the port number of the web sever.
Enter Value [default=23015]
>23015

Specify the port number for RMI communications.
Enter Value [default=1099]
>1099

Specify the installation directory path name of Storage Navigator Modular (for Web).
   Caution: Make sure that the specified installation directory
              path name ends with a forward slash (/).
   Caution: Replace backslashes (\) with forward slashes (/)
              in the specified installation directory path name.

Enter Value [default=C:/Program Files/Storage Navigator Modular Web/]
```

```

>D:/Storage Navigator Modular Web/

Launch setup has successfully completed.

You must restart the Device Manager Server and Common Component Services for this
these changes to take effect.

Exit - Default is n?(y, n):

```

9.1.3 Deleting Launch Settings

Delete the launch environment settings by using the simple setup tool `launchapptool`.

You can delete the launch settings if the `launchapp.properties` file and `httpsd.conf` file reside in the installation folder and are write-enabled.

Note: For details on the `launchapp.properties` file, see section 8.10.

Note: The `httpsd.conf` file is stored in the following location:

- In Windows:

installation-folder-for-HiCommand-Suite-Common-Component\httpsd\conf

- In Solaris or Linux:

/opt/HiCommand/Base/httpsd/conf

1. To delete the launch environment settings, execute the following command from the command prompt or terminal window:

- In Windows:

installation-folder-for-the-Device-Manager-server\HiCommandServer\tools\launchapptool.bat

The following shows an example of executing the command:

```

C:\Program
Files\HiCommand\DeviceManager\HiCommandServer\tools\launchappto
ol.bat

```

- In Solaris or Linux:

```
# /opt/HiCommand/HiCommandServer/tools/launchapptool.sh
```

2. The main menu appears. Select **3**.

A deletion confirmation message appears.

```

=====
launchapptool
=====

1) Storage Navigator Modular (for Web) launch setup
2) Disk Array Management Program (for Web) launch setup
3) Delete launch settings
4) Exit

>3

Launch settings will now be deleted.

Would you like to delete launch settings?(y, n):y

```

3. Select **y** if you are sure you want to delete the launch environment settings; select **n** to cancel deletion.
4. Restart the Device Manager server and HiCommand Suite Common Component. For Windows, see section 3.5; for Solaris or Linux, see section 4.6.

The launch environment settings are now deleted.

```
Launch settings have successfully been deleted.
```

```
You must restart the Device Manager Server and Common Component Services  
for this these changes to take effect.
```

```
Exit - Default is n?(y, n):
```

9.1.4 Accessing a Storage Subsystem with Password Protection or Account Authentication

Enabled

For storage subsystems whose Password Protection or Account Authentication is enabled, do not use a user ID that starts with "HDvM".

When Password Protection or Account Authentication is enabled, if you launch the Storage Navigator Modular (for Web), the system creates a temporary user account for the Storage Navigator Modular (for Web) to access the storage subsystem. This user account is automatically registered into the system with a user ID that starts with "HDvM", and automatically deleted after you exit the Storage Navigator Modular (for Web). Therefore, manual registration of a user account that starts with "HDvM" or making changes of the registration details might cause the launch to fail.

9.2 Linking With DAMP (for Web)

This section describes prerequisites and environment setup for linking with DAMP (for Web). This section also describes storage subsystem information to be registered into DAMP (for Web).

Caution: The Linux version does not support linkage with DAMP (for Web).

9.2.1 Prerequisites for Using DAMP (for Web)

The prerequisites for using DAMP (for Web) are as follows:

- To perform DAMP launching, the DAMP (for Web) version must be 10.00 or later.
- For details on the environment requirements for running DAMP (for Web), see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.
- Install DAMP (for Web) on the machine where the HiCommand Device Manager server is installed.
- To use DAMP (for Web), the settings for the Web server for running DAMP (for Web) are required.

- Use HiCommand Suite Common Component for a Web server for running DAMP (for Web). HiCommand Suite Common Component is installed during installation of the Device Manager server.
- DAMP (for Web) cannot be used together with Storage Navigator Modular (for Web), and cannot be used while the TagmaStore AMS/WMS series is in use.

Caution: The web server for DAMP (for Web) can be accessed via only one NIC even if multiple NICs are installed on the machine. To link with DAMP (for Web) in a machine environment where multiple NICs are installed, you need to specify the NIC to be used to access the web server for DAMP (for Web). The IP address or host name specified for this setting must be the same as that specified during installation of the Device Manager server. For details on how to specify the settings, see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.

Caution: To link with DAMP (for Web) in a cluster environment, the host you specify for accessing DAMP's Web server must be identical to the logical host name you specified when installing the Device Manager server. For details on setting the host name, see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.

Caution: When the Password Protection functionality is enabled on Thunder 9200 or Thunder 9500V Series, DAMP (for Web) operations launched from Physical View, Web Client operations[#], or CLI operations[#], might fail. The following are ways to avoid this problem:

- Change the application you use from DAMP (for Web) to Storage Navigator Modular (for Web).
- Use DAMP (for Web) by directly connecting to it from the browser.

When you connect to DAMP (for Web), you must use a user ID different from the one you used when you registered Thunder 9200 or Thunder 9500V in Device Manager.

In this case, you cannot perform DAMP (for Web) operations and operations for Web Client or CLI[#] at the same time for the same storage subsystem (Thunder 9200 or Thunder 9500V). This however is the normal situation when the Password Protection functionality is enabled.

- Stop the polling of the Device Manager server, and try not to perform DAMP (for Web) operations and operations for Web Client or CLI[#] at the same time for the same storage subsystem (Thunder 9200 or Thunder 9500V).

To stop the polling of the Device Manager server:

1. Specify 0 for `server.dispatcher.daemon.pollingPeriod` property in the `dispatcher.properties` file. For details about the `server.dispatcher.daemon.pollingPeriod` property, see section 8.5.4.
2. To enable the property settings, restart the Device Manager server.

This operation disables the alert detection performed by polling. However, for the following storage subsystems, you can use alert detection by using the SNMP trap:

- TagmaStore USP
- Lightning 9900V Series

- Lightning 9900 Series

#: Includes such operations as changing the configuration of, or refreshing the storage subsystem, by using Web Client or CLI.

9.2.2 Setting the Launch Environment When Using DAMP (for Web)

Set the launch environment for DAMP (for Web) using the simple setup tool `launchapptool`.

The following conditions apply when setting the launch environment:

- The `launchapp.properties` file and `httpsd.conf` file must exist in the installation folder and must be write-enabled.
- HiRDB must be running.

Note: For details on the `launchapp.properties` file, see section 8.10.

Note: The `httpsd.conf` file is stored in the following location:

- In Windows:
`installation-folder-for-HiCommand-Suite-Common-Component\httpsd\conf`
- In Solaris:
`/opt/HiCommand/Base/httpsd/conf`

Note: For details on how to check the HiRDB operating status and start the HiRDB service, see section 5.2.1.

To specify launch environment settings for DAMP (for Web):

1. Install DAMP (for Web).

For details on how to install DAMP (for Web), see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.

2. Execute the following command from the command prompt or terminal window:

- In Windows:
`installation-folder-for-the-Device-Manager-server\HiCommandServer\tools\launchapptool.bat`

The following shows an example of executing the command:

```
C:\Program
Files\HiCommand\DeviceManager\HiCommandServer\tools\launchapptool.bat
```

- In Solaris:
`# /opt/HiCommand/HiCommandServer/tools/launchapptool.sh`

3. The main menu appears. Select **2**.

```
=====
launchapptool
=====
```

```

1) Storage Navigator Modular (for Web) launch setup
2) Disk Array Management Program (for Web) launch setup
3) Delete launch settings
4) Exit

```

```
>3
```

Launch settings will now be deleted.

```
Would you like to delete launch settings?(y, n):y
```

4. If launch environment settings already exist for DAMP (for Web), a confirmation message asks if you want to change the current settings. Select **y** to change the settings, or **n** to leave the settings unchanged.
5. Specify the protocol to be used in the Web server URL. Select **1** to use http protocol, or **2** to use https protocol.

Specify the URL protocol.

- ```

1) http
2) https

```

Caution: To use https, settings to enable SSL communication with the web server must be specified in advance.

Enter Value [default=1]

```
>1
```

**Caution:** For option **2**, the Web server must be set up for SSL communication.

6. Enter the IP address or host name to be used in the Web server's URL.

Specify an IP address or host name that can be accessed from the client machine on which the Web Client program is running.

Specify the IP address or hostname of the web server.

Enter Value [default=10.208.64.134]

```
>10.208.64.134
```

**Note:** To use a local host, specify its IP address rather than the host name.

7. Enter the port number to be used in the Web server's URL.

Specify the port number of the web server.

Enter Value [default=23015]

```
>23015
```

8. Enter the installation directory of DAMP (for Web).

Specify the installation directory path name of Disk Array Management Program (for Web).

Caution: Make sure that the specified installation directory path name ends with a forward slash (/).

Caution: Replace backslashes (\) with forward slashes (/) in the specified installation directory path name.

Enter Value [default=C:/Program Files/DA Manager Web/]

```
>C:/Program Files/DA Manager Web/
```

**Caution:** Make sure that the path ends with a forward slash (/).

**Caution:** In Windows, replace \ with / in the path name.

Example: "C:/Program Files/DA Manager Web/"

9. Restart the Device Manager server and HiCommand Suite Common Component. For Windows, see section 3.6; for Solaris or Linux, see section 4.7.

The changes to the launch environment settings now apply.

Launch setup has successfully completed.

You must restart the Device Manager Server and Common Component Services for these changes to take effect.

Exit - Default is n?(y, n):

10. Check whether DAMP (for Web) runs on HiCommand Suite Common Component. Specify the following URL in the browser, and then make sure that the DAMP (for Web) window appears.

`http://host-name-or-IP-address:portID/program/DeviceManager/damp/default.htm`

11. Refresh the storage subsystems to be operated on by DAMP (for Web).

**Note:** If you set up the launch environment by using the simple setup tool, the URL associated with DAMP (for Web) is set as alias information in HiCommand Suite Common Component. This alias information remains if you subsequently uninstall Device Manager or DAMP (for Web). To delete the alias information and other launch settings, see section 9.1.3.

### 9.2.3 Storage Subsystem Information to be Registered by Using DAMP (for Web)

- To operate storage subsystems by launching DAMP (for Web) from the HiCommand Device Manager server, the storage subsystem information must be registered in advance by using DAMP (for Web). For details on how to register this information, see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.
- To register a unit name of the storage subsystem by using DAMP (for Web), use an IP address with an H added as a prefix. (Example: If the IP address is 192.168.108.123, the unit name will be H192.168.108.123.)
- The IP address used for a unit name is *IP-address-1* or *IP-address-2* with which the storage subsystem was registered in HiCommand Device Manager.
- When DAMP (for Web) is directly used without launching DAMP (for Web) after the launch settings for DAMP (for Web) are configured, specify the following URL in the browser.

`http://host-name-or-IP-address:portID/program/DeviceManager/damp/default.htm`

This way, you can also register information about storage subsystems.

## 9.3 Starting HSSM From the Dashboard

To link with HSSM and start HSSM from the **Dashboard** menu, create the `StorageServicesManager.conf` file in the following folder if the file has not been created yet. The location of this file differs depending on the OS:

In a Windows system:

`HiCommand-Suite-Common-Component-installation-folder\common`

In a Solaris system or a Linux system:

`/opt/HiCommand/Base/common`

In the `StorageServicesManager.conf` file, specify the `LaunchURL` parameter in the format shown as follows:

#### Format of the `StorageServicesManager.conf` File

```
LaunchURL=HSSM-URL
```

In *HSSM-URL*, specify the URL used to start HSSM. For details about this URL, see the HSSM documentation.

For example, if the name of the HSSM management server is *machinename*, configure the `StorageServicesManager.conf` as follows:

#### For Secure Connections:

```
LaunchURL=https://machinename
```

#### For Nonsecure Connections:

```
LaunchURL=http://machinename
```



## Chapter 10 Troubleshooting

- Problems and Solutions (see section 10.1)
- Collecting Maintenance Information (see section 10.2)

### 10.1 Problems and Solutions

Table 10.1 lists the common problems and solutions after installing Device Manager on a Windows, Solaris, or Linux platform. For a listing of Device Manager Error Codes, see *Hitachi HiCommand Device Manager Error Codes* (MK-92HC016).

Table 10.1 General Troubleshooting Information

| Problem                                                                                                                                                                                                                                                                                                                                                                                                              | Solution                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>DESCRIPTION: Inconsistencies in LUNs and Logical Group information. LUNs disappear or logical group information is inconsistent between Device Manager Servers.</p> <p>CAUSE: Multiple Device Manager Servers are managing the storage subsystems.</p>                                                                                                                                                            | <p>SOLUTION: Never have more than one active Device Manager Server managing a single storage array at a time. Device Manager was designed to manage multiple storage arrays, but not to cooperate with other instances of Device Manager Server to manage the same storage subsystems.</p> <p>More than one active Device Manager client is not a problem.</p> |
| <p>DESCRIPTION: Not enough disk space for installation in a Windows environment.</p> <p>CAUSE: The InstallAnywhere installer needs sufficient space to unpack the compressed installation files. InstallAnywhere uses the Windows TEMP environment variable to locate the temporary directory for extracting the files. You should have at least 100 MB of free space available, preferably more, on this drive.</p> | <p>SOLUTION: Choose a different drive and directory, or delete files from the Windows TEMP directory to clear enough space for InstallAnywhere.</p>                                                                                                                                                                                                            |
| <p>DESCRIPTION: Incompatibility between Graph-Track 4.06 and Device Manager, such that installing one over the other can cause failures.</p> <p>CAUSE: Device Manager requires InterBase (GDS32.dll) at core rev level 6.0.1.0 and Graph-Track 4.06 uses core rev level 5.6.0.29.</p>                                                                                                                                | <p>SOLUTION: Upgrade to Graph-Track 5.0 or higher. If you are running Graph-Track 4.06, please see Graph-Track Alert # 21 for installation instructions.</p>                                                                                                                                                                                                   |
| <p>DESCRIPTION: Inconsistencies in LUNs and Logical Group information. LUNs disappear or logical group information is inconsistent between the Device Manager Servers.</p> <p>CAUSE: Multiple Device Manager Servers are managing the storage arrays.</p>                                                                                                                                                            | <p>SOLUTION: Never have more than one active Device Manager Server managing a single storage array at a time. Device Manager was designed to manage multiple storage arrays, but not to cooperate with other instances of the Device Manager Server to manage the same storage array.</p> <p>More than one active Device Manager client is not a problem.</p>  |

| Problem                                                                                                                                                                                                                                                                                                                                                            | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>DESCRIPTION: The InterBase Server service stops and then the HiCommandServer service stops when an attempt is made to start the HiCommand Device Manager server on a machine managed by the Microsoft Systems Management Server (SMS).</p> <p>CAUSE: The InterBase Server and SMS are not set to coexist in the current configuration.</p>                      | <p>SOLUTION: To prevent the InterBase Server service from stopping, change the following SMS settings file:</p> <pre>SMS-installation-directory\Inboxes\Clifiles.src\Hinv\ Sms_def.mof</pre> <p>Change the settings (change TRUE to FALSE) as follows:</p> <p>Before change:</p> <pre>[SMS_Report(TRUE),   SMS_Group_Name("Services"),   ResID(5000),ResDLL("SMS_RXPL.dll"),   SMS_Class_ID("MICROSOFT SERVICE 1.0")] class Win32_Service : SMS_Class_Template&lt;BR/&gt;</pre> <p>After change:</p> <pre>[SMS_Report(FALSE),   SMS_Group_Name("Services"),   ResID(5000),ResDLL("SMS_RXPL.dll"),   SMS_Class_ID("MICROSOFT SERVICE 1.0")] class Win32_Service : SMS_Class_Template&lt;BR/&gt;</pre> <p>For details, see WORKAROUND in the following Microsoft knowledge base article:<br/> <i>Microsoft Knowledge Base Article - 257509 SMS: Hardware Inventory May Cause Third-Party Win32 Services to Stop</i><br/> <a href="http://support.microsoft.com/default.aspx?scid=kb;EN-US;257509">http://support.microsoft.com/default.aspx?scid=kb;EN-US;257509</a></p> |
| <p>DESCRIPTION: The following message was displayed during Device Manager server installation on a Linux environment:</p> <pre>[yyyy/mm/dd hh:mm:ss] main() Invoke: /opt/HiCommand/HiCommandServer/inst/GetDBInfo.sh ... An error occurred during loading of a library. ... CAUSE: The prerequisite library compat-libstdc++-33-3.2.3-47.3 is not installed.</pre> | <p>SOLUTION: Perform the following operations in order:</p> <p>Install <code>compat-libstdc++-33-3.2.3-47.3</code>.</p> <p>Uninstall the Device Manager server (see section 4.10).</p> <p>Perform a new installation of the Device Manager server (see section 4.4).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



| Problem                                                                                                                                                                                                                                                                                               | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>DESCRIPTION:</b> An error occurs during Device Manager server installation.</p> <p><b>CAUSE:</b> There is an error in the environment or settings on the installation destination machine.</p>                                                                                                  | <p><b>SOLUTION:</b> If an error occurs during Device Manager server installation, perform the following:</p> <p>Use the <code>hcmdsgetlogs</code> command to collect maintenance information<sup>#1</sup>.</p> <p>Back up the database and property files if they have not been backed up already<sup>#2</sup>. If other HiCommand Suite products are installed, refer to the documentation of the appropriate product when performing backup.</p> <p>In the <b>Applications</b> tab of the Windows Task Manager, terminate the <b>InstallAnywhere</b> task. If other applications are currently being installed, wait until installation of all applications has been completed before terminating the <b>InstallAnywhere</b> task.</p> <p>Reboot the system.</p> <p>In Windows, delete the following folders if they exist:</p> <p>The folder set for the <code>temp</code> environment variable of the installation user:</p> <pre>{1345FCD1-713E-4449-8F76-3F6503941040}</pre> <p><b>Example:</b> <code>C:\Documents and Settings\Administrator\Local Settings\Temp\{1345FCD1-713E-4449-8F76-3F6503941040}</code></p> <p>The following folder directly under the startup drive:</p> <pre>_HDBInstallerTemp</pre> <p><b>Example:</b> <code>C:\_HDBInstallerTemp</code></p> <p>Folders within the installation folder of the Device Manager server:</p> <pre>installation-folder-for-the-Device-Manager-server\_InstallerFilesTemp</pre> <p>Perform one of the following, based on the type of installation:</p> <p>When an attempt to perform a new installation fails:</p> <p>Perform uninstallation. Reboot the system, and then install again.</p> <p>When an attempt to perform an upgrade installation fails:</p> <p>Perform uninstallation. Reboot the system, and then perform a new installation again. Then, restore any backed-up data <sup>#3</sup>.</p> <p>When an attempt to update the database fails during an upgrade installation from version 3.5 or earlier:</p> <p>Perform the recovery procedures that follow the troubleshooting information.</p> <p><sup>#1</sup> For details about collecting maintenance information, see section 10.2.</p> <p><sup>#2</sup> For details about performing backup manually, see section 3.2.3 for Windows, or section 4.4.2 for Solaris™ or Linux. For details about using commands to back up a database, see section 3.7.1 for Windows, or section 4.8.1 for Solaris™ or Linux.</p> <p><sup>#3</sup> For details about using commands to restore a database, see section 3.7.2 for Windows, or section 4.8.2 for Solaris™ or Linux.</p> |
| <p><b>DESCRIPTION:</b> In an upgrade operation of the Device Manager Server 3.5 or earlier to 4.0 or later, an error occurred while a database is being converted.</p> <p><b>CAUSE:</b> The free disk space used to store the database is less than 100 MB, or a required service is not running.</p> | <p><b>SOLUTION:</b> Make sure the following:</p> <p>100 MB of free disk space is available for the Device Manager Server database.</p> <p>The Common Component is running.</p> <p>Both InterBase and InterClient are running.</p> <p>If no problem was found, execute the database convert command (<code>migrateFmIB</code>). For details about the database convert command, see section 3.4.1 for Windows, or section 4.5.6 for Solaris.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <p><b>DESCRIPTION:</b> In an operation to upgrade the HiCommand Device Manager server version 3.5 or earlier to version 4.0 or later, an error occurred before the database was converted.</p>                                                                                                        | <p><b>SOLUTION:</b> Perform the following operations in sequence and then retry the installation:</p> <p>Copy the following files to a location other than the installation folder:</p> <p>In Windows:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Problem                                                                             | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CAUSE: Installation was interrupted due to service interruption, or other failures. | <p><i>installation-folder-for-the-Device-Manager-server\migrateFmIB.bat</i></p> <p><i>installation-folder-for-the-Device-Manager-server\HiCommandServer\ext\interclient.jar</i></p> <p><i>installation-folder-for-the-Device-Manager-server\HiCommandServer\database\interbase\HICOMMAND.GDB</i></p> <p>Among the property files below, copy only those in which a value other than the default value is specified for a property:</p> <p><i>installation-folder-for-the-Device-Manager-server\HiCommandServer\config\*.properties</i></p> <p><i>installation-folder-for-the-Device-Manager-server\SupportTools\CollectTool\TIA.properties</i></p> <p><i>installation-folder-for-the-Device-Manager-server\HiCommandCLI\legacy\R2.1\HiCommandCLI.properties</i></p> <p><i>installation-folder-for-the-Device-Manager-server\HiCommandCLI\legacy\R2.0\HiCommandCLI.properties</i></p> <p><i>installation-folder-for-the-Device-Manager-server\HiCommandCLI\HiCommandCLI.properties</i></p> <p>In Solaris</p> <p><i>/opt/HiCommand/migrateFmIB.sh</i></p> <p><i>/opt/HiCommand/HiCommandServer/ext/interclient.jar</i></p> <p><i>/opt/HiCommand/HiCommandServer/database/interbase/HiCommand.gdb</i></p> <p>/ Among the property files below, copy only those in which a value other than the default value is specified for a property:</p> <p><i>/opt/HiCommand/HiCommandServer/config/*.properties</i></p> <p><i>/opt/HiCommand/SupportTools/CollectTool/TIA.properties</i></p> <p><i>/opt/HiCommand/HiCommandCLI/legacy/R2.1/HiCommandCLI.properties</i></p> <p><i>/opt/HiCommand/HiCommandCLI/legacy/R2.0/HiCommandCLI.properties</i></p> <p><i>/opt/HiCommand/HiCommandCLI/HiCommandCLI.properties</i></p> <p>Uninstall the HiCommand Device Manager server.</p> <p>Perform a new installation of the HiCommand Device Manager server (for details, see section 3.2.2 for Windows, or section 4.4 for Solaris™).</p> <p><b>Note:</b> For Windows, choose the same directory as the original installation directory.</p> <p>Copy the files <i>migrateFmIB.bat</i> (sh), <i>interclient.jar</i>, and <i>hicommand.gdb</i>, copied in the first step, back to the original location.</p> <p>Also copy <i>interclient.jar</i> to the following directory:</p> <p>In Windows:</p> <p><i>installation-folder-for-HiCommand-Suite-Common-Component\database\interclient.jar</i></p> <p>In Solaris:</p> <p><i>/var/opt/HiCommand/Base/database/interclient.jar</i></p> <p>Apply the same settings specified in the property files that were copied in the first step to the relevant property files (if *.properties.old have already been created, simply copy them).</p> <p>Use the following procedure to start HiCommand Suite Common Component.</p> <p>In Windows:</p> |

| Problem                                                                                                                                                                                                                             | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                     | <p>Execute the following command from the command prompt:</p> <pre>installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdssrv /start</pre> <p>The following shows an example of executing the command:</p> <pre>C:\Program Files\HiCommand\Base\bin\hcmdssrv /start</pre> <p>In Solaris:</p> <p>Execute the following command from the terminal window:</p> <pre># /opt/HiCommand/Base/bin/hcmdssrv -start</pre> <p>Execute the database convert command (migrateFmIB)</p> <p>Set the <code>server.base.initialsynchro</code> property to true.</p> <p>Use the following procedure to start the HiCommand Device Manager server.</p> <p>In Windows:</p> <p>Select <b>Start</b>, <b>Programs</b>, <b>HiCommand</b>, <b>Device Manager</b>, and then <b>Start Server</b>.</p> <p>In Solaris:</p> <p>Execute the following command from the terminal window:</p> <pre># /opt/HiCommand/suitesrvctl -start_hdvm</pre> <p>If Tuning Manager has been installed in a different server and the Single Sign On function is used, configure the settings for Single Sign On again (see the Tuning Manager manual).</p> <p>If the port for HiCommand Suite Common Component has been changed, return the setting to that state.</p>                                                                               |
| <p><b>DESCRIPTION:</b> As a result of a Device Manager server upgrade, the user ID or password is no longer usable.</p> <p><b>CAUSE:</b> The user ID or password contains a character that cannot be used in version 3.5 later.</p> | <p><b>SOLUTION:</b> Perform the following operations in sequence and create a new user ID or password.</p> <p>Back up <code>oldDbBackup.gbk</code>. <code>oldDbBackup.gbk</code> in the following location:</p> <p>In Windows:</p> <pre>installation-folder-for-the-Device-Manager-server\HiCommandServer\database\interbase\oldDbBackup.gbk</pre> <p>In Solaris:</p> <pre>/opt/HiCommand/HiCommandServer/database/interbase/oldDbBackup.gbk</pre> <p>Uninstall the HiCommand Device Manager server).</p> <p>Re-install the HiCommand Device Manager server used before the upgrade (see the manual of the installed version).</p> <p>Restore <code>oldDbBackup.gbk</code> (which was backed up in the first step).</p> <p>Create a new user by using the appropriate characters for user IDs in version 3.5 or later. The following characters are usable:</p> <p>User ID:</p> <pre>A-Z a-z 0-9 - _ . @ + #</pre> <p>Password:</p> <pre>A-Z a-z 0-9 ! # \$ % &amp; ( ) * + - . = @ \ ^ _   ' "</pre> <p>Upgrade the HiCommand Device Manager server (for details see section 3.2.3 for Windows, or section 4.4.2 for Solaris™).</p> <p>Clear the cache in Java Web Start.</p> <p>For details about how to clear the cache in Java Web Start, see the <i>HiCommand Device Manager Web Client User's Guide</i>.</p> |

| Problem                                                                                                                                                                                                                                                                                                                                                                             | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>DESCRIPTION: In Windows, reports are not displayed when the HTML button is clicked in the Storage Utilization by Host - Reports subwindow or Storage Utilization by Logical Group - Reports subwindow in the Web Client.</p> <p>CAUSE: Either too many storage subsystems have been selected, or the size of the memory heap used by the Device Manager server is too small.</p> | <p>SOLUTION: Decrease the number of storage subsystems selected in the Storage Utilization by Host - Reports subwindow or Storage Utilization by Logical Group - Reports subwindow, and then display a report. Alternatively, increase the size of the memory heap used by the Device Manager server to allow reports to be displayed.</p> <p>The size of the memory heap can be changed as follows.</p> <p>Edit the <code>HiCommandServer.lax</code> file in the following folder to change the memory heap size:</p> <p><i>Installation-folder-for-the-Device-Manager-server\HiCommandServer</i></p> <p>Open the <code>HiCommandServer.lax</code> file in a text editor, and change the value for <code>lax.nl.java.option.java.heap.size.max</code> to the value calculated below, in bytes. The default value is 268,435,456 (256 MB). If the result of the following formula is already smaller than 256 MB, then no changes are needed.</p> <p><math>(15000 \times \text{number-of-LUNs-displayed} + 1700 \times \text{number-of-WWNs-displayed}) \times \text{number-of-users}</math></p> <p><i>number-of-LUNs-displayed</i>: Total number of LUNs displayed per host (not the number of LUNs set for the storage subsystem)</p> <p><i>number-of-WWNs-displayed</i>: Total number of WWNs displayed per LUN</p> <p><i>number-of-users</i>: Number of users using the report feature concurrently.</p> <p>After the <code>HiCommandServer.lax</code> file is changed, perform the following to restart the Device Manager server.</p> <p>Select Start, Programs, HiCommand, Device Manager, and then Stop Server.</p> <p>After the Device Manager server has been stopped, select Start, Programs, HiCommand, Device Manager, and then Start Server.</p> |

| Problem                                                                                                                                                                                                                                                                                                                                                                                          | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>DESCRIPTION: In Solaris or Linux, reports are not displayed when the HTML button is clicked in the Storage Utilization by Host - Reports subwindow or the Storage Utilization by Logical Group - Reports subwindow in the Web Client.</p> <p>CAUSE: Either too many storage subsystems have been selected, or the size of the memory heap used by the Device Manager server is too small.</p> | <p>SOLUTION: Decrease the number of storage subsystems selected in the Storage Utilization by Host - Reports subwindow or Storage Utilization by Logical Group - Reports subwindow, and then display a report. Alternatively, increase the size of the memory heap used by the Device Manager server to allow reports to be displayed.</p> <p>The size of the memory heap can be changed as follows.</p> <p>Edit the <code>hicommand.sh</code> file in the following folder to change the memory heap size:</p> <pre>/opt/HiCommand</pre> <p>Open the <code>hicommand.sh</code> file in a text editor, and change the value of the <code>-Xmx</code> option of the <code>java</code> command specified in the <code>start</code> option script to the value calculated below, in MB. The default value is 256 MB. If the result of the following formula is already smaller than 256 MB, then no changes are needed.</p> $(0.0145 \times \text{number-of-LUNs-displayed} + 0.00165 \times \text{number-of-WWNs-displayed}) \times \text{number-of-users}$ <p><i>number-of-LUNs-displayed</i>: Total number of LUNs displayed per host (not the number of LUNs set for the storage subsystem)</p> <p><i>number-of-WWNs-displayed</i>: Total number of WWNs displayed per host</p> <p><i>number-of-users</i>: Number of users using the report feature concurrently.</p> <p>The following shows how to change the value for a value of 512 MB as calculated above.</p> <p>Before: <code>java -Xmx256m -classpath ...</code></p> <p>After: <code>java -Xmx512m -classpath ...</code></p> <p>After the <code>hicommand.sh</code> file is changed, perform the following to restart the Device Manager server.</p> <p>Execute the following command:</p> <pre># /opt/HiCommand/suitesrvctl -stop_hdvm</pre> <p>After the Device Manager server has been stopped, execute the following command:</p> <pre># /opt/HiCommand/suitesrvctl -start_hdvm</pre> |
| <p>DESCRIPTION: Database registration attempts fail when the Device Manager server is installed in a Windows cluster environment.</p> <p>CAUSE: The termination code of the <code>hcmsdbclustersetup</code> command is 250 (data import processing has failed).</p>                                                                                                                              | <p>SOLUTION: Perform the following procedures in the order given to restore the system.</p> <p>If the database has been backed up:</p> <p>Perform recovery from the database backup.</p> <p>To restart setting of the cluster environment, first perform the procedures to stop the Device Manager server and HiCommand Suite Common Component.</p> <p>If the database has not been backed up:</p> <p>Execute the following two commands to restore the state of Device Manager.</p> <pre>installation-folder-for-HiCommand-Suite-Common-Component\HDB\BIN\pdntcmd.bat</pre> <pre>installation-folder-for-HiCommand-Suite-Common-Component\HDB\BIN\pdrels -r HDVM_RD</pre> <p>The following shows examples of executing the commands:</p> <pre>C:\Program Files\HiCommand\Base\HDB\BIN\pdntcmd.bat</pre> <pre>C:\Program Files\HiCommand\Base\HDB\BIN\pdrels -r HDVM_RD</pre> <p>Uninstall the Device Manager server.</p> <p>Install the Device Manager server.</p> <p>Restart setting of the cluster environment.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Problem                                                                                                                                                                                                                                                                                                                                                                                               | Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>DESCRIPTION: Database registration attempts fail when the Device Manager server is installed in Solaris or Linux: cluster environment.</p> <p>CAUSE: The termination code of the <code>hcmdsdbclustersetup</code> command is 250 (data import processing has failed).</p>                                                                                                                          | <p>SOLUTION: Perform the following procedures in the order given to restore the system.</p> <p>If the database has been backed up:<br/>Perform recovery from the database backup.</p> <p>To restart setting of the cluster environment, first perform the procedures to stop the Device Manager server and HiCommand Suite Common Component.</p> <p>If the database has not been backed up:<br/>Execute the following two commands to restore the state of Device Manager.</p> <pre># /opt/HiCommand/Base/HDB/bin/pduxenv # /opt/HiCommand/Base/HDB/bin/pdrels -r HDVM_RD</pre> <p>Uninstall the Device Manager server.</p> <p>Install the Device Manager server. For details about how to perform the installation, see section 4.4.</p> <p>Restart setting the cluster environment.</p> |
| <p>DESCRIPTION: SSL communication with SMI-S Provider is disabled because SSL configuration for SMI-S failed during Device Manager server installation.</p> <p>CAUSE: An unexpected error occurred while configuring SSL for SMI-S.</p>                                                                                                                                                               | <p>SOLUTION: Use the <code>HiKeytool</code> command to configure SSL for SMI-S. For details about how to do this, see section 7.4.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p>DESCRIPTION: The service discovery feature is not available, because the SLP service (or the SLP daemon) failed to start during Device Manager server installation.</p> <p>CAUSE: An unexpected error occurred during the SLP service (or the SLP daemon) startup.</p>                                                                                                                             | <p>SOLUTION: Set the service discovery feature. For details about how to do this, see section 11.5.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <p>DESCRIPTION: Canceling the SLP service (or the SLP daemon) failed during Device Manager server uninstallation.</p> <p>CAUSE: This problem happens in either of the following cases:</p> <p>When performing uninstallation while the SLP service (or the SLP daemon) is running</p> <p>When performing uninstallation while the SLP service is stopped, but is registered as a Windows service.</p> | <p>SOLUTION: Stop or clear the SLP service (or the SLP daemon). For details about how to do this, see section 11.5.</p> <p>If you use Windows, the OpenSLP file might be deleted during uninstallation. In that case, perform the following operations in order, and then clear the SLP service:</p> <p>In the Services panel, disable the Service Location Protocol service.</p> <p>Restart Windows.</p>                                                                                                                                                                                                                                                                                                                                                                                 |
| <p>DESCRIPTION: Even though the port number of SMI-S was entered during Device Manager server installation, after installation, the Device Manager server does not start or communication with SMI-S Provider is disabled.</p> <p>CAUSE: The port number entered during installation is incorrect.</p>                                                                                                | <p>SOLUTION: Change the port number used by the CIM/WBEM features, and then restart the Device Manager server.</p> <p>For details about how to change port numbers, see section 11.3.2.2 When you change a port number, do not specify the port numbers described in section 5.5.1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Problem                                                                                                                                                                                                                                                                                                                                         | Solution                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>DESCRIPTION: Device Manager output the message KAIC00114-E An attempt to start the HTTP server on port "2001" failed. Or KAIC00115-E An attempt to start HTTPS server on port "2443" failed. to the application log and the system log, and then could not be started.</p> <p>CAUSE: The port number is already used by another program.</p> | <p>SOLUTION: Change the port number used by the Device Manager web server (2001) or the port number used for secure HTTP communication by the Device Manager web server (2443), and then restart the Device Manager server.</p> <p>For details on how to change a port number, see sections 8.2.2 and 8.2.3. When changing a port number, do not specify the port numbers listed in section 5.4.1.</p> |

## 10.2 Collecting Maintenance Information

When an error occurs in a Device Manager Server, you can use the **hcmdsgetlogs** command to obtain the maintenance information required for analyzing the Device Manager Server error.

### 10.2.1 Using hcmdsggetlogs to Acquire Log Files

The **hcmdsggetlogs** command collects the log file, and has the following format:

For Windows:

**installation-directory-for-Common-Component\Bin\hcmdsggetlogs /dir directory-name [/type application-name] [/arc archive-file-name]**

The following shows an example of executing the command:

**C:\Program Files\HiCommand\Bin\hcmdsggetlogs /dir C:\hcmds\_logs /type DeviceManager /arc dvm\_log1**

For Solaris or Linux:

**# /opt/HiCommand/Base/bin/hcmdsggetlogs -dir directory-name [-type application-name] [-arc archive-file-name]**

- *dir directory-name* specifies the name of the directory on a local disk that stores the log file.
- *type application-name* specifies the name of the application from which the log file will be collected. To collect the Device Manager log file, specify *DeviceManager* as the application name. If you do not specify the application type, all of the Web applications registered in HiCommand Common Component are applicable.
- *arc archive-file-name* specifies the name of the archive file to be created. If you do not specify this parameter, the default is *HiCommand\_log*. When the archive file name is output, it will have a .jar extension.
- Return values

- 0: Normal termination
- 1: Parameter error
- 2: Abnormal termination

For example, when the OS is Windows, and you are collecting only the Device Manager log, the command would be:

```
installation-directory-for-Common-Component\bin\hcmdsgetlogs /dir desired-directory /type DeviceManager
```

When the OS is Solaris or Linux:, and you are collecting only the Device Manager log, the command would be:

```
/opt/HiCommand/Base/bin/hcmdsgetlogs -dir desired-directory -type DeviceManager
```

When the OS is Windows, and you are collecting the log of a HiCommand Suite product in the hicmd\_log file, the command would be:

```
installation-directory-for-Common-Component\bin\hcmdsgetlogs /dir desired-directory /arc hicmd_log
```

When the OS is Solaris or Linux:, and you are collecting the log of a HiCommand Suite product in the hicmd\_log archive file, the command would be:

```
/opt/HiCommand/Base/bin/hcmdsgetlogs -dir desired-directory -arc hicmd_log
```

The **hcmdsgetlogs** command has the following features:

- When you execute the **hcmdsgetlogs** command, the content of the directory specified with the **dir** option must be empty. If the directory specified with the **dir** option does not exist, the **hcmdsgetlogs** command creates the directory.
- Set the write permission of the directory specified with the **-dir** option so that files can be created in the directory.
- The **hcmdsgetlogs** command acquires the log files and database. If you execute the command, four archive files (**.jar**, **.hdb.jar**, **.db.jar**, and **.csv.jar**) are created.
- Do not run more than one **hcmdsgetlogs** command simultaneously.
- To execute the **hcmdsgetlogs** command, you must log on as a user who has the Administrator permissions or as the root user.
- In the **arc** option, do not use a character that is not permitted for a file name by the OS. In Solaris or Linux, do not specify a path that includes a space.
- In the **dir** option, do not use a character that is not permitted for a directory name by the OS. In Solaris or Linux, do not specify a path that includes a space.

### 10.2.2 Obtaining a Thread Dump

If Device Manager uses the HBase Storage Mgmt Common Service function, collect a Java VM thread dump to check the cause of the problem if one of the following events occurs:



- The Device Manager log on window is not displayed when you start Web Client.
- The Device Manager main window is not displayed after logging on to Device Manager.
- The Device Manager main window is not displayed when you start a Device Manager Server from Tuning Manager.

To acquire a Java VM thread dump:

Windows:

- a) In **<installation directory>\cc\web\containers\HiCommand**, create a file called **dump**.

Access the **Services** panel.

Stop the HBase Storage Mgmt Common Service. see section 5.2.2 if you need instructions.

The javacorexxx.xxxx.txt file is output to  
**<installation directory>\cc\web\containers\HiCommand**.

From the **Services** panel, start the HBase Storage Mgmt Common Service.

Solaris or Linux:

- a) Execute **kill -3** PID. PID is a process ID written in the  
**/var/opt/HiCommand/Base/CC/web/containers/HiCommand/logs/cjstdout.log** file.

The **jvacorexxx.xxxx.txt** file is output to  
**/opt/HiCommand/Base/CC/web/containers/HiCommand**.

Stop the HBase Storage Mgmt Common Service process using the following command:

**# /opt/HiCommand/Base/bin/hcmdssrv -stop -server HBase**

Start the Storage Mgmt Common Service. see section 5.2.1 if you need instructions.

### 10.3 Contacting the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including the circumstances surrounding the error or failure, and the exact content of any error messages.

The worldwide Hitachi Data Systems Support Centers are:

- Hitachi Data Systems North America/Latin America  
San Diego, California, USA  
1-800-348-4357
- Hitachi Data Systems Europe  
Contact Hitachi Data Systems Local Support
- Hitachi Data Systems Asia Pacific  
North Ryde, Australia  
61-2-9325-3300



# Chapter 11 Overview and Setup of CIM/WBEM

This chapter gives an overview of CIM/WBEM (Web-Based Enterprise Management) provided by Device Manager, and explains how to set up CIM/WBEM.

- Device Manager and CIM/WBEM (see section 11.1)
- CIM/WBEM Features of Device Manager (see section 11.2)
- Preparations for Operating the CIM/WBEM Features (see section 11.3)
- Properties File Settings When Executing CIM (see section 11.4)
- Setting the Service Discovery Feature (see section 11.5)
- User Permissions for Using CIM/WBEM Features (see section 11.6)

## 11.1 Device Manager and CIM/WBEM)

Device Manager supports WBEM defined by the standards-setting organization DMTF. WBEM is a standard proposed by the DMTF for managing networked devices, including hosts and storage subsystems, over the Internet. WBEM enables you to share data about devices in different environments (such as environments with different vendors, operating systems, or protocols) without considering the differences. WBEM is based on CIM, an object-oriented information model.

CIM, defined by DMTF, is a standardized approach for managing systems in network environments. CIM provides a framework for expressing the data to be managed. Applying CIM to storage subsystems enables you to use standardized methods to manage the configuration and status of storage subsystems in networks.

The CIM models provided by Device Manager conform to the SMI-S specifications (SNIA-CTP) endorsed by SNIA. The CIM models of the Device Manager server are defined in MOF (Managed Object Format) files provided by Device Manager. The MOF namespace provided by Device Manager.

CIM clients can access Device Manager by using the CIM XML/HTTP interface defined by WBEM.

Figure 11.1 shows the CIM components for Device Manager.

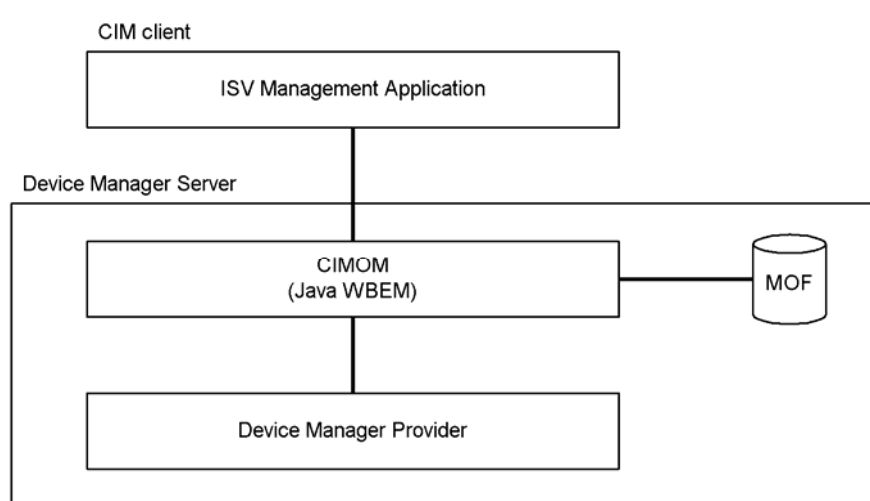


Figure 11.1 CIM Components for Device Manager

From a CIM client, you can specify a namespace by using the follow procedure:

- Specify the Device Manager version.  
Specify `root/hitachi/dmxx` (xx is an abbreviation for the version number).  
For example, to specify version 5.5, enter `root/hitachi/dm55`.
- Specify the SMI-S version.  
Specify `root/smis/smisxx` (xx is an abbreviation for the version number).  
For example, to specify version 1.1.0, enter `root/smis/smis11`.  
The latest namespaces that complies with the specified SMI-S version is selected.
- Specify the condition `current`.  
Enter `root/smis/current`.  
The current namespace is selected.

The following table lists and describes the correspondence between the namespaces supported by Device Manager and SMI-S versions.

Table 11.1 Correspondence Between Namespaces and SMI-S Versions

| Namespace          |                     |                      | SMI-S |
|--------------------|---------------------|----------------------|-------|
| <code>dmXX#</code> | <code>smisXX</code> | <code>current</code> |       |
| <code>dm35</code>  | --                  | --                   | 1.0.2 |
| <code>dm40</code>  | --                  | --                   |       |
| <code>dm41</code>  | --                  | --                   |       |
| <code>dm42</code>  | <code>smis10</code> | --                   |       |
| <code>dm43</code>  | --                  | --                   | 1.1.0 |
| <code>dm50</code>  | --                  | --                   |       |

|      |        |         |  |
|------|--------|---------|--|
| dm51 | --     | --      |  |
| dm55 | smis11 | current |  |

Legend:

--: N/A

#: If you need to specify the namespaces (dm24 and dm30) that were supported by versions of Device Manager earlier than 5.5, contact the maintenance personnel.

You can obtain information about CIM at:

<http://www.dmtf.org/home/>

You can obtain information about SMI-S at:

<http://www.snia.org/smi/home/>

## 11.2 CIM/WBEM Features of Device Manager

CIM/WBEM of Device Manager provides the three features specified in SMI-S:

- Objection operation feature
- Indication feature
- Service discovery feature

These features are described below:

### Object operation feature

The SMI-S specifications, which Device Manager conforms to, define the interfaces for devices that make up a storage network, such as storage subsystems, virtual storage systems, switches, and hosts. The features that need to be provided by the management service to manage the devices are grouped in a profile for each device.

The profiles used by the CIM/WBEM features of Device Manager are the Array profile and its subprofiles. The Array profile defines the interfaces for storage subsystems.

### Indication feature

The *indication* feature is the event notification feature defined by CIM. When an event occurs in a CIM server, the CIM server reports the indication instance, which shows the information about the event (such as generation or deletion of a CIM instance), to CIM clients. For a CIM client to receive indications, its location and transmission conditions for indications must be registered in the CIM server beforehand. For details on how to register, see the SNIA website.

Device Manager reports the occurrence of the following events:

- Generation of a volume
- Deletion of a volume
- Allocation of a path

- Cancellation of a path

#### Service discovery feature

Device Manager provides the service discovery feature based on the Service Location Protocol (SLP).

The SLP is undergoing standardization by IETF and provides a way to discover desired services available in a network. For details on the SLP, see RFC2608.

Just by specifying the type of service, SLP clients can obtain information (such as URLs) about how to access the available services, and information about service attributes.

In Device Manager, the Device Manager server uses the SLP to report information about the WBEM Service.

### 11.3 Preparations for Operating the CIM/WBEM Features

CIM/WBEM features are disabled by default in the Device Manager settings. To use the CIM/WBEM features, you must specify the following settings after installation:

- Basic settings required to use the CIM/WBEM features
- Setting the port used by CIM/WBEM features
- Settings required to use SSL (Secure Sockets Layer) in the CIM/WBEM features

#### 11.3.1 Basic Settings Required to Use the CIM/WBEM Features

To use the CIM/WBEM features, you must first enable them.

To enable the CIM/WBEM features:

1. Change the setting in the Device Manager server property file.

Change the setting of the `server.cim.support` property in the property file `server.properties` from `false` to `true`. The `server.properties` file is stored in the following location:

In Windows:

*installation-folder-for-the-Device-Manager-server*\HiCommandServer\config\

**Note:** The default installation folder for Device Manager server is as follows:

C:\Program Files\HiCommand\DeviceManager

In Solaris or Linux:

/opt/HiCommand/HiCommandServer/config

2. Stop any service that uses a port having a port number used by the CIM/WBEM service.

The table below shows the port used by each CIM/WEB feature.

Table 11.2 Port Number Used by CIM/WBEM Features

| Feature                     | Port number used                                                                   |
|-----------------------------|------------------------------------------------------------------------------------|
| Objection operation feature | For non-SSL communication: 5988 (default)<br>For SSL communication: 5989 (default) |
| Service discovery feature   | 427                                                                                |

Execute the following command to determine if any service program running is using the same port to be used by each CIM/WBEM feature:

- In Windows: `netstat -anp TCP`
- In Solaris: `netstat -an -P tcp`
- In Linux: `netstat -tan`

If any service program using the same port is running, change the port number for the service program.

If any service program is running (normally, another WBEM service program) that is using the same port to be used by an object operation feature, the object operation feature is not available.

If any service program is running (normally, another SLP service (or SLP daemon)) that uses the same port (427) to be used by the service discovery feature, an attempt to start the SLP service (or SLP daemon) for Device Manager will fail.

In Solaris:

In Solaris, CIMOM is incorporated in the system during installation. If CIMOM is running, an attempt to start CIM/WBEM might fail.

Use the following command to stop CIMOM:

```
/etc/init.d/init.wbem stop
```

Also, delete CIMOM from `inittab` to prevent CIMOM from automatically starting.

### 3. Set up and start the SLP service (or SLP daemon).

Set up the SLP service (or SLP daemon) to enable the service discovery feature. For details about how to set up this feature, see section 11.5.

**Note:** In the SLP service (or SLP daemon), register the port used by CIM/WBEM features by default. For the ports used by CIM/WBEM features, see section 11.3.2.

### 4. Restart the HiCommand Device Manager server.

In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.

When the Device Manager server has stopped, select **Start, Programs, HiCommand, Device Manager**, and then **Start Server**.

In Solaris or Linux:

Execute the following command:

```
/opt/HiCommand/suitesrvctl -stop_hdvm
```

When the Device Manager server has stopped, execute the following command:

```
/opt/HiCommand/suitesrvctl -start_hdvm
```

**Note:** When upgrading Device Manager from version 4.2 or earlier to 4.3 or later, check the `httpsd.conf` file. If this file contains a description that enables SSL functionality in the CIM/WBEM features, remove the description before performing the upgrade. The `httpsd.conf` file is stored in the following folder or directory:

In Windows:

*installation-folder-for-HiCommand-Suite-Common-Component*\httpsd\conf\httpsd.conf

In Solaris or Linux:

`/opt/HiCommand/Base/httpsd/conf/httpsd.conf`

Coding that enables SSL:

```
LoadModule proxy_module complete-path-name-for-the-proxy-module

Listen port-number-for-SSL-in-CIM/WBEM-features
<VirtualHost host-name:port-number-for-SSL-in-CIM/WBEM-features>
 ServerName host-name
 SSLEnable
 SSLRequireSSL
 SSLCertificateFile complete-path-name-for-the-certificate-file-from-CA
 SSLCertificateKeyFile complete-path-name-for-the-private-key-file
 ProxyPass / http://127.0.0.1:5988/
 ProxyPassReverse / http://127.0.0.1:5988/
</VirtualHost>
```

## 11.3.2 Setting up the Ports Used by CIM/WBEM Features

### 11.3.2.1 Opening and closing ports according to the communication type

Ports can be opened or closed according to the communication type used by CIM/WBEM features. Security can be enhanced by closing unused ports.

To open or close the port:

1. Using the `server.cim.support.protocol` property in the property file (`server.properties`) of the Device Manager server, set up whether to open or close each port according to the communication type.

The setting values for `server.cim.support.protocol` are shown in the table below.

Table 11.3 Setting Values for `server.cim.support.protocol`

| Setting value | Port status |            | Applicable communication type |
|---------------|-------------|------------|-------------------------------|
|               | HTTP port   | HTTPS port |                               |
| 1             | Open        | Close      | Non-SSL communication         |
| 2             | Close       | Open       | SSL communication             |



|   |      |      |                                             |
|---|------|------|---------------------------------------------|
| 3 | Open | Open | SSL communication and non-SSL communication |
|---|------|------|---------------------------------------------|

- Restart the Device Manager server.

In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.

When the Device Manager server has stopped, select **Start, Programs, HiCommand, Device Manager**, and then **Start Server**.

In Solaris or Linux:

Execute the following command:

```
/opt/HiCommand/suitesrvctl -stop_hdvm
```

When the Device Manager server has stopped, execute the following command:

```
/opt/HiCommand/suitesrvctl -start_hdvm
```

### 11.3.2.2 Changing the port number

In the initial state, the port numbers used by the CIM/WBEM features are as follows:

- HTTP port number: 5988
- HTTPS port number: 5989

To specify the port number, follow the steps below:

- Change the port number set in the Device Manager server property file (`server.properties`). For details on the Device Manager server property file, see section 11.4.1.

To change the HTTP port number:

Change the port number set in `server.cim.http.port`.

To change the HTTPS port number:

Change the port number set in `server.cim.https.port`.

- Restart the HiCommand Device Manager server.

In Windows:

Select **Start, Programs, HiCommand, Device Manager**, and then **Stop Server**.

When the Device Manager server has stopped, select **Start, Programs, HiCommand, Device Manager**, and then **Start Server**.

In Solaris or Linux:

Execute the following command:

```
/opt/HiCommand/suitesrvctl -stop_hdvm
```

When the Device Manager server has stopped, execute the following command:

```
/opt/HiCommand/suitesrvctl -start_hdvm
```

## 11.4 Properties File Settings When Executing CIM

When executing CIM, you must set up the properties files for the Device Manager server and restart Device Manager. The following table lists the Device Manager server properties you must set.

Table 11.4 Properties You Must Set for Device Manager Server When Executing CIM

| Settings required                                      | File name               | Property                             |
|--------------------------------------------------------|-------------------------|--------------------------------------|
| Enable CIM, and specify ports used in CIM              | server.properties       | server.cim.support                   |
|                                                        |                         | server.cim.support.protocol          |
|                                                        |                         | server.cim.http.port                 |
|                                                        |                         | server.cim.https.port                |
| Set up the operating environment for the WBEM Service. | wbemservices.properties | classpath                            |
|                                                        |                         | BaseDir                              |
|                                                        |                         | propdir                              |
|                                                        |                         | logdir                               |
| Set the authentication class for Device Manager.       | cimom.properties        | org.wbemservices.wbem.cimom.pswdprov |

### 11.4.1 The server.properties File

When executing CIM, set up the following properties in addition to the regular settings.

#### 11.4.1.1 server.cim.support

This property specifies whether to use the CIM interface. Set the `server.cim.support` property to `true`. The default is `false`, which specifies that the CIM interface is not used.

```
whether the server supports CIM interface or not
server.cim.support={true | false}
```

#### 11.4.1.2 server.cim.support.protocol

Specify whether to open or close the port used by the CIM interface.

Default: 3 (opens both the port for SSL communication and port for non-SSL communication.)

#### 11.4.1.3 server.cim.http.port

To use non-SSL for the CIM interface, specify the HTTP port number.

Default: 5988

#### 11.4.1.4 server.cim.https.port

To use SSL for the CIM interface, specify the port number of HTTPS.

Default: 5989

### 11.4.2 The jserver.properties File

This properties file sets up the operating environment for the WBEM Service. This file is stored in the following directory when Device Manager is installed:

In Windows:

`installation-folder-for-the-Device-Manager-server\HiCommandServer\config`

**Note:** The default installation folder for Device Manager server is as follows:

`C:\Program Files\HiCommand\DeviceManager`

In Solaris or Linux:

`/opt/HiCommand/HiCommandServer/config`

The contents of the `wbemservices.properties` file are as follows.

#### 11.4.2.1 classpath

This property sets `classpath` required for operating the WBEM Service. Do not change the value of this property.

#### 11.4.2.2 BaseDir

This property specifies the name of the base directory of `classpath` required for operating the WBEM Service. Do not change the value of this property.

#### 11.4.2.3 propdir

This property specifies the directory containing the `cimom.properties` file. Do not change the value of this property.

#### 11.4.2.4 logdir

This property specifies the directory containing the repository (compilation results of the MOF file: `store`). Do not change the value of this property.

#### 11.4.3 Saving the cimom.properties File

Save the `cimom.properties` file in the directory specified by the `propdir` property in the `wbemservices.properties` file.

##### 11.4.3.1 org.wbemservices.wbem.cimom.pswdprov

This property specifies the authentication class for Device Manager. Do not change the value of this property.

#### 11.5 Setting the Service Discovery Feature

This section describes how to set the service discovery feature of Device Manager. To use the service discovery feature of Device Manager, you need the following prerequisite software:

In Windows or Linux:

OpenSLP 1.0.11

OpenSLP is attached to Device Manager. When you install Device Manager, the required file is copied. For details on OpenSLP, see the OpenSLP website (<http://www.openslp.org/>).

In Solaris:

SUNWslpr package and SUNWslpu package

These packages are attached to the Solaris system. For details on the SUNWslpr package and the SUNWslpu package, see the Sun Microsystems website (<http://docs.sun.com/>).

OpenSLP, the SUNWslpr package, and the SUNWslpu package need to be set up separately. For the setup procedure, see section 11.5.1.

When starting the CIM client, set the language tag (locale) for the service discovery feature to English (en).

## 11.5.1 Setting Up the Service Discovery Feature

### 11.5.1.1 In Windows

When you install Device Manager, the OpenSLP file is copied simultaneously. To use the service discovery feature, you need to register the SLP service (service name: `slpd`, display name: `Service Location Protocol`) as a Windows service. Perform the following procedure to register the SLP service as a Windows service.

To register the SLP service:

1. Install Device Manager, and then log on as a member of the Administrator group.
2. Display the command prompt and move to the folder containing the OpenSLP executable file.

OpenSLP is installed in the following folder:

```
installation-folder-for-the-Device-Manager-server\HiCommandServer\wsi\bin\windows
```

**Note:** The default installation folder for Device Manager server is as follows:

```
C:\Program Files\HiCommand\DeviceManager
```

3. Register the SLP service as a Windows service.

Execute the following command:

```
> slpd -install
```

To automatically start the service when Windows starts, execute the command with the `auto` option.

```
> slpd -install auto
```

This operation is required only once. Even if you restart the Windows system, you do not need to re-register the daemon. If you execute the command without the `auto` option, you need to manually start the SLP service.

If the following message is displayed when Device Manager is uninstalled, release the SLP service manually from the Windows services.

```
An attempt to release the SLP service has failed. After uninstallation, release the SLP service manually. Uninstallation continues.
```

To release the SLP service:

1. Log on as a member of the Administrator group.
2. Show the command prompt and move to the folder containing the OpenSLP executable file.
3. Release the SLP service from Windows services.

Execute the following command:

```
> slpd -remove
```

### 11.5.1.2 In Solaris

In Solaris, the SLP daemon is installed in the standard configuration. However, the SLP daemon does not become active with the default settings. Perform the following procedure to automatically start the SLP daemon when the system starts.

To automatically start the SLP daemon:

1. Log on as the root user.

2. Check that the SLP daemon is installed.

Use the `pkginfo` command or the graphical user interface of Solaris to check that the `SUNWslpr` package and the `SUNWslpu` package are installed. If they are not installed, install them.

3. Change the name of the configuration file of the SLP daemon.

Change the file name as follows:

Before change: `/etc/inet/slp.conf.example`

After change: `/etc/inet/slp.conf`

4. Start the SLP daemon.

Restart Solaris or execute the following command:

```
/etc/init.d/slpd start
```

If Device Manager is uninstalled, stop or cancel the SLP daemon, as required. You can cancel the SLP daemon by using either of the following methods:

- Delete `/etc/init.d/slpd` or rename it.
- Delete `/etc/inet/slp.conf` or rename it.

### 11.5.1.3 In Linux

When Device Manager is installed, the OpenSLP file is copied at the same time. Settings do not need to be specified after installation, and the service discovery feature can be used as is.

If the following message is displayed when Device Manager is uninstalled, release the SLP daemon manually from the Linux daemons manually.

```
WARNING: An attempt to release the SLP daemon has failed. After uninstallation,
release the SLP daemon manually. Uninstallation continues.
```

To release the SLP daemon:

1. Log on as the root user.

2. Stop the SLP daemon.

Execute the following command:

```
/opt/HiCommand/HiCommandServer/wsi/bin/slpd.sh stop
```

3. If `/etc/init.d/slpd` exists, delete it.

Execute the following command:

```
chkconfig --level 01345 slpd off
chkconfig --del slpd
rm -f /etc/init.d/slpd
```

## 11.5.2 Starting and Stopping the Service Discovery Feature

### 11.5.2.1 In Windows

To manually start the SLP service, perform either of the following procedures:

- From **Administrative Tools**, choose **Services** and then **Service Location Protocol** to start the SLP service.
- Show the command prompt, move to the folder containing the OpenSLP executable file, and execute the following command:

```
> slpd -start
```

To stop the SLP service, perform either of the following:

- From **Administrative Tools**, choose **Services** and then **Service Location Protocol**.
- Display the command prompt, move to the folder containing the OpenSLP executable file, and execute the following command:

```
> slpd -stop
```

### 11.5.2.2 In Solaris

To manually start the SLP daemon, execute the following command:

```
/etc/init.d/slpd start
```

To stop the SLP daemon, execute the following command:

```
/etc/init.d/slpd stop
```

**Note:**

Sometimes, the `/etc/init.d/slpd stop` command may not successfully stop the SLP daemon. In that case, perform the following procedure to stop the SLP daemon:

- Return the name of the `/etc/inet/slp.conf` file to `/etc/inet/slp.conf.example`.  
You must delete the `/etc/inet/slp.conf` file at this point.
- Restart Solaris.

### 11.5.2.3 In Linux

To manually start the SLP daemon, execute the following command:

```
/opt/HiCommand/HiCommandServer/wsi/bin/slpd.sh start
```

To stop the SLP daemon, execute the following command:

```
/opt/HiCommand/HiCommandServer/wsi/bin/slpd.sh stop
```

### 11.5.3 Notes on Using OpenSLP

The SLP service (or SLP daemon) of OpenSLP outputs operation logs to the following file:

In Windows:

```
%WINDIR%\slpd.log#
```

#%WINDIR% is replaced by the value of the environment variable WINDIR in Windows. Normally, the value is C:\WINNT\.

In Linux:

```
/opt/HiCommand/HiCommandServer/wsi/cfg/slp.log
```

By default, only the start message at SLP service startup is output to the log file. Since the SLP service log output (or SLP daemon) accumulates as time elapses, if you use the SLP service (or SLP daemon) for an extended period of time, the log output may eventually use up a lot of disk space. To prevent this, you need to periodically back up the log file and clear the disk space.

## 11.6 User Permissions for Using CIM/WBEM Features

The following table shows the user permissions for using CIM/WBEM features, based on the Device Manager permissions and executable CIM methods.



Table 11.5 User Permissions for Using CIM/WBEM Features

| # | Resource group               | Device Manager permissions |        |      |      | Executable CIM methods |                |
|---|------------------------------|----------------------------|--------|------|------|------------------------|----------------|
|   |                              | Admin                      | Modify | View | Peer | Service methods        | CIM operations |
| 1 | All Resources                | Yes                        | Yes    | Yes  | --   | Permitted              | Permitted      |
| 2 |                              | --                         | Yes    | Yes  | --   | Permitted              | Permitted      |
| 3 |                              | --                         | --     | Yes  | --   | Not permitted          | Permitted      |
| 4 |                              | --                         | --     | --   | Yes  | Not permitted          | Permitted      |
| 5 | User-defined resource groups | Yes                        | Yes    | Yes  | --   | Not permitted          | Not permitted  |
| 6 |                              | --                         | Yes    | Yes  | --   | Not permitted          | Not permitted  |
| 7 |                              | --                         | --     | Yes  | --   | Not permitted          | Not permitted  |
| 8 |                              | --                         | --     | --   | Yes  | Not permitted          | Permitted      |

Legend:

Yes: Has corresponding Device Manager permissions

--: Does not have corresponding Device Manager permissions

Permitted: Execution of corresponding CIM methods is permitted

Not permitted: Execution of corresponding CIM methods is not permitted

For *Peer* Device Manager permissions, users are treated as All Resources users, even when they belong to a user-defined resource group, due to Device Manager server processing.



## Chapter 12 Overview and Setup of VDS

This chapter provides an overview of Device Manager VDS Provider, and explains the setup procedure.

- About Device Manager VDS Provider (see section 12.1)
- Installation Requirements and Procedures (see section 12.2)
- Operating Device Manager VDS Provider (see section 12.3)

### 12.1 About Device Manager VDS Provider

#### 12.1.1 Overview of Device Manager VDS Provider

Windows Server 2003 provides Virtual Disk Service (VDS), which is a virtual disk system designed to manage storage subsystem devices via standardized interfaces.

Device Manager VDS Provider is a Device Manager software product that provides and configures storage subsystem information for VDS.

Device Manager VDS Provider supports the following OSs:

- Windows Server 2003 (with Service Pack 1)  
For Enterprise Edition or Datacenter Edition, IPF (running on WOW64) is supported.
- Windows Server 2003 x64 Edition  
Only EM64T (running on WOW64) is supported.
- Windows Server 2003 R2

#### 12.1.2 Functions of Device Manager VDS Provider

Device Manager VDS Provider is a hardware provider that is resident on a Windows host and replies to VDS requests. Device Manager VDS Provider provides functions for:

- Obtaining the following storage subsystem related configuration information:
  - Subsystem
  - LUN
  - LUN replication information
  - Path information
  - Port information
- Performing the following storage subsystem related configuration tasks:
  - LUN creation
  - LUN expansion

- LUN deletion
- LUN mapping
- LUN masking

Before you can use the DISKRAID command provided by Microsoft, you must perform the following installation tasks:

- Install Device Manager VDS Provider.  
**Important:** To use Device Manager VDS Provider, you need to change the value of the Device Manager server property `server.cim.support` to `true` in the `server.properties` file, and then restart the Device Manager server.
- If your host computer OS is not Windows Server 2003 R2, download VDS SDK from the Microsoft web page (<http://www.microsoftstoragepartners.com/>) and then install it.

### 12.1.3 Available Functions in Storage Manager for SANs for Windows Server 2003 R2

You can operate a storage subsystem via the VDS Provider function of Device Manager by using Storage Manager for SANs provided by Windows Server 2003 R2.

The following functions are available:

- Create LUN
- Delete LUN
- Extend LUN
- Rename LUN
- Assign LUN
- Unassign LUN
- Manage Server Connections
- Rename Subsystem
- Refresh

The following functions are not available:

- Blink Drive Light
- Manage iSCSI Targets
- Manage iSCSI Security
- Log On to iSCSI Targets

## 12.2 Installation Requirements and Procedures

### 12.2.1 Installing Device Manager VDS Provider

There are three methods for installing Device Manager VDS Provider in Windows.

- **New installation**  
Use this installation method to install Device Manager VDS Provider in a host in which Device Manager VDS Provider does not exist.
- **Upgrade installation (to update an earlier version)**  
Use this installation method to install Device Manager VDS Provider in a host in which version 4.2, 4.3, 5.0, or 5.1 of Device Manager VDS Provider is installed.
- **Re-installation (to correct the same version)**  
Use this installation method to install Device Manager VDS Provider in a host in which version 5.5 of Device Manager VDS Provider is installed.

You can obtain the version of an installed Device Manager VDS Provider by executing the following command:

```
installation-folder-for-Device-Manager-VDS-Provider\bin\hdmvinfo.exe
```

The following shows an example of executing the command:

```
C:\Program Files\HITACHI\HDvM_VDS\bin\hdmvinfo.exe
```

**Notes:** Note the following when installing Device Manager VDS Provider:

- At least 5 MB of free space is required on the hard disk. Also, an additional 5 MB of free space is required on the system drive to create temporary files during installation.
- After installation, you will need to set up access permission for the Device Manager VDS provider installation folder. Since access permission cannot be set for FAT or FAT32 formatted drives, be sure to install Device Manager VDS provider installation on an NTFS formatted drive.
- Do not execute the Microsoft-provided DISKRAID or `hdmvconfig` command during an upgrade installation of Device Manager VDS Provider. Also, do not install Device Manager VDS Provider when the Microsoft-provided DISKRAID or `hdmvconfig` command is being executed. If you execute the above command during an upgrade installation, the installation might end before completion. Make sure that you restart the system after installation
- Version 4.1 or earlier of Device Manager VDS Provider is automatically installed or uninstalled when Device Manager Agent is installed. If you want to use version 4.1 or earlier of Device Manager VDS Provider, install Device Manager Agent. For details on how to install Device Manager Agent, see the *HiCommand Device Manager Agent Installation Guide*.
- Version 4.1 or earlier of Device Manager VDS Provider cannot be used at the same time as version 4.2 or later. Stop the service of the version that will not be used. For details on how to stop the service, see section 12.3.1. The service names are:

- In version 4.1 or earlier: **Hitachi RAID Provider**
- In version 4.2 or later: **Device Manager VDS Provider**
- If the Hitachi RAID Provider service is running, version 4.3 or later of Device Manager VDS Provider cannot be installed. If you attempt to install it, the following message appears.

Hitachi RAID Provider is running. Re-install after stopping this service.

- Overwrite installation (an update installation or a fixed version) may fail, in which case cancellation of the overwrite installation is reported. Overwrite installation (update or fixed) may also fail when the startup status of the Device Manager VDS Provider service is disabled. In this case, reboot the system, and then perform installation again.

### 12.2.1.1 New installation

To perform a new installation:

1. Log on to Windows using an Administrators-group user ID.
2. Insert the Device Manager VDS Provider CD-ROM.  
**Note:** Before starting the installation, cancel any programs that may be running.
3. From the **Start** menu, select **Run**. In the displayed panel, click **Browse**. In the displayed tree view, select `setup.exe` (in the \VDS folder on the CD-ROM). Then, click **OK**.  
 The Welcome to the InstallShield Wizard for Device Manager VDS Provider panel appears.
4. Select **Next**.  
 The Device Manager VDS Provider License Agreement panel appears.
5. Select **Next**.  
 The Choose Destination Location panel appears. Select the folder in which you want Device Manager VDS Provider to be installed.  
**Note:** Do not select the installation folder for Device Manager VDS Provider version 4.1 or earlier.  
**Note:** The installation folder displayed by default differs for x86, and IPF or EM64T.
  - For x86  
     \Program Files\HITACHI\HDvM\_VDS
  - For IPF and EM64T  
     \Program Files (x86)\HITACHI\HDvM\_VDS
6. Select **Next**.  
 The IP Address of the Device Manager server panel appears.  
 Enter the IP address of the Device Manager server.
7. Select **Next**.  
 The Installation Confirmation panel appears.

**Note:** In this and previous steps, you can select **Cancel** to cancel installing Device Manager VDS Provider.

8. Select **Install**.

The Progress Panel appears.

When installation is complete, a panel indicating the completion of installation appears.

9. Select **Finish**.

10. Set up access permissions for the installation folder for Device Manager VDS provider installation folder.

Using the appropriate OS function, set up read/write access permissions for the Administrators group and SYSTEM group.

Do not set up access permissions for groups other than the Administrators group and SYSTEM group.

If your installation has ended normally, specify your user ID and password for connection to the Device Manager server. For details on how to specify your user ID and password, see section 12.3.3.

#### 12.2.1.2 Upgrade Installation (To Update an Earlier Version)

To perform an upgrade installation:

1. Log on to Windows using an Administrators-group user ID.

2. Insert the Device Manager VDS Provider CD-ROM.

**Note:** Before starting the installation, cancel any programs that may be running.

3. From the **Start** menu, select **Run**. In the displayed panel, click **Browse**. In the displayed tree view, select `setup.exe` (in the \VDS folder on the CD-ROM). Then, click **OK**.

The Welcome to the InstallShield Wizard for Device Manager VDS Provider panel appears.

4. Select **Next**.

**Note:** In this and previous steps, you can select **Cancel** to cancel installing Device Manager VDS Provider.

The Progress Panel appears.

When installation is complete, a panel indicating the completion of installation appears.

5. Select **Finish**.

6. Set up access permissions for the Device Manager VDS provider installation folder.

Using the appropriate OS function, set up read/write access permissions for the Administrators group and SYSTEM group.

Do not set up access permissions for groups other than the Administrators group and SYSTEM group.

**Note:** Upgrade installation relies on the already specified Device Manager server IP address, user ID, and password as they are inherited from the original system. If you want to change the IP address, user ID, or password, see section 12.3.3.

### 12.2.1.3 Re-installation (To Correct the Same Version)

To perform an upgrade installation:

1. Log on to Windows using an Administrators-group user ID.
2. Insert the Device Manager VDS Provider CD-ROM. Then, from the **Start** menu, select **Run**. In the displayed panel, click **Browse**. In the displayed tree view, select `setup.exe` (in the \VDS folder on the CD-ROM), and then click **OK**.

A window is displayed in which Repair or Remove can be selected.

**Note:** You can also perform the above operation by choosing **Start, Settings, Control Panel**, and **Add or Remove Programs**. In the displayed panel, select **Device Manager - VDS Provider** and then click the **Change/Remove** button.

3. Select **Repair** and choose **Next**.

The setup dialog box is displayed.

4. Select **Next**.

A dialog box indicating that preparations for setup have finished is displayed.

**Note:** Up until this step, you can select **Cancel** to cancel installation of Device Manager VDS Provider.

5. Select **Next**.

A dialog box appears, indicating that Device Manager VDS Provider is being installed, and then a panel indicating the completion of installation appears.

6. Select **Finish**.

7. Set up access permissions for the Device Manager VDS provider installation folder.

Using the appropriate OS function, set up the read/write access permissions for the Administrators group and SYSTEM group.

Do not set up access permissions for groups other than the Administrators group and SYSTEM group.

### 12.2.2 Uninstalling Device Manager VDS Provider

This section describes how to uninstall Device Manager VDS Provider.

**Note:** When you perform an uninstallation under the following conditions, a message that prompts you to restart the system is displayed after the uninstallation. Even though this message appears, you do not have to restart the system. Take the appropriate action by following the relevant instructions.

- If the exe file or bat file corresponding to Device Manager VDS Provider is being executed:

Stop the exe file or bat file (or both) that is being executed.

- If the command prompt window is open and its current folder is the same as the installation folder for Device Manager VDS Provider:

Close the command prompt window.



Uninstalling Device Manager VDS Provider stops service programs and deletes all the folders, files, and registry information that were registered during installation. The system returns to the status before installation.

**Note:** Once uninstallation is started, you cannot use the **Cancel** button to stop the processing. After the uninstallation finishes, install Device Manager VDS Provider again.

To uninstall Device Manager VDS Provider (method 1):

1. Select **Start, Settings, Control Panel**, and **Add/Remove Programs**.
2. Click the **Remove** button for Device Manager VDS Provider.

To uninstall Device Manager VDS Provider (method 2):

1. Select **Start, Settings, Control Panel**, and **Add/Remove Programs**.
2. Click the **Change** button for Device Manager VDS Provider.

The Device Manager - VDS Provider maintenance menu is displayed.

3. Click the **Remove** button.

**Caution:** When changes or deletions are performed from **Add/Remove Programs**, an error might occur, in which case the following message is displayed. If an error occurs, use `setup.exe` in the `\VDS` folder on the CD-ROM to perform any changes or deletions.

An error occurred during reading C:\Program Files\Common Files\InstallShield\Professional\RunTime\10\50\Intel32\Ctor.dll. The specified module cannot be found.

## 12.3 Operating Device Manager VDS Provider

### 12.3.1 Starting and Stopping Device Manager VDS Provider

The following describes how to start and stop Device Manager VDS Provider.

#### 12.3.1.1 Starting the service

Open the Services window by choosing **Start, Settings, Control Panel, Management Tools**, and then **Services**. Then, start the **Device Manager VDS Provider** service.

**Note:** After the service starts, the message KAIC24804-I is output to the log file:

KAIC24804-I Inquiring storage information from Device Manager Server has been completed.

The log file is:

`installation-folder-for-Device-Manager-VDS-Provider\logs\hdmvcomm.log`

**Caution:** Do not connect from the VDS client to the VDS Provider until the Device Manager VDS Provider service starts.

### 12.3.1.2 Stopping the service

Open the Services window by choosing **Start, Settings, Control Panel, Management Tools,** and then **Services**. Then, stop the **Device Manager VDS Provider** service.

### 12.3.1.3 Notes on Starting and Stopping the Service

After stopping or restarting Device Manager VDS Provider while the DISKRAID command is running, if the subcommand of the DISKRAID command is executed, an error occurs. In this case, finish the DISKRAID command by executing the `QUIT` command, and then restart the DISKRAID command.

Device Manager VDS Provider acquires information about the storage subsystems from the Device Manager server when Device Manager VDS Provider starts, or the `REFRESH` subcommand of the DISKRAID command is executed.

It might take a long time to acquire this information, so follow the directions below:

- Notes on restarting Device Manager VDS Provider

Until Device Manager VDS Provider completes processing to acquire configuration information about the storage subsystems, note that:

- If you execute a DISKRAID command to display information about the storage subsystems, the information is not displayed.
- If you execute the `REFRESH` subcommand of the DISKRAID command, an error occurs.

- Notes on executing the `REFRESH` subcommand of the DISKRAID command

Until Device Manager VDS Provider completes processing to acquire configuration information about the storage subsystem, note that:

- If you execute a DISKRAID command to display information about the storage subsystems, the information before the refresh operation is displayed.
- If you re-execute the `REFRESH` subcommand of the DISKRAID command, an error occurs.

**WARNING:** If the `REFRESH` subcommand is executed, while the storage subsystem deleted from the Device Manager server is selected by executing the `SELECT` subcommand, the `LIST` subcommand might display incorrect information. In such a case, select another storage subsystem by executing the `SELECT` subcommand, and then re-execute the `REFRESH` subcommand, or restart the DISKRAID command.

### 12.3.2 Device Manager VDS Provider Property Files

Device Manager VDS Provider uses two property files:

- `vds.properties` file

This file is used to configure the Device Manager VDS Provider environment.

- `logger.properties` file

This file is used to configure the Device Manager VDS Provider logging function.

These files are stored in the following locations:

`vds.properties` file:

*installation-folder-for-Device-Manager-VDS-Provider\config\vds.properties*

`logger.properties` file:

*installation-folder-for-Device-Manager-VDS-Provider\config\logger.properties*

**WARNING:** If you change the contents of the Device Manager VDS Provider property files (`vds.properties` and `logger.properties`), you must restart the service.

### 12.3.2.1 `vds.properties` file

The `vds.properties` file contains the following information:

- IP address of the Device Manager server
- Account (user name and password) used for Device Manager VDS Provider
- Port number of the Device Manager server

You can change the above information after installing Device Manager VDS Provider. For details on how to change the information, see section 12.3.3.

### 12.3.2.2 `logger.properties` File

The `logger.properties` file is used to configure the logging function of Device Manager VDS Provider. Table 12.1 contains the logging function properties of Device Manager VDS Provider.

Table 12.1 `logger.properties` File

| Property                     | Description                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>logger.loglevel</code> | You can specify the log level for data that Device Manager VDS Provider outputs to the files <code>hdvmmcomm.log</code> and <code>hdvmmprov.log</code> .<br>Log levels: DEBUG, INFO, WARN, ERROR, and FATAL.<br>Default: INFO |

| Property              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| logger.MaxBackupIndex | <p>You can specify the maximum number of log file backups. If more log files are generated than specified, Device Manager VDS Provider writes over the oldest one. If a log file reaches the maximum size, the file is renamed by adding a counter (which represents the version) to the file name. For example, <code>hdvmcomm.log</code> becomes <code>hdvmcomm.log.1</code>. If additional backup log files are created, the counter increases until the specified number of backup log files is generated (for example, <code>hdvmcomm.log.1</code> becomes <code>hdvmcomm.log.2</code>). After the specified number of backup log files are created, each time a new backup file is created, the oldest backup file is deleted.</p> <p>Specifiable range: 1 through 20.</p> <p>Default: 10</p> |
| logger.MaxFileSize    | <p>You can specify the maximum size of each log file. If a log file becomes larger than the specified maximum, Device Manager VDS Provider creates a new file and writes logs to it. Unless <code>KB</code> is specified for kilobytes or <code>MB</code> for megabytes, a specified size is interpreted to mean bytes. Specifiable range: from 512KB to 32MB</p> <p>Default: 1 MB</p>                                                                                                                                                                                                                                                                                                                                                                                                              |

**Caution:** If you changed the `logger.properties` file, restart Device Manager VDS Provider.

### 12.3.3 Changing Device Manager VDS Provider Settings

Use the `hdvmconfig` command to change the information about Device Manager VDS Provider specified in the `vds.properties` file.

To change an account used in Device Manager VDS Provider, use Web Client to create a user ID in advance. For details on how to create a user ID, see the *HiCommand Device Manager Web Client User's Guide*.

The `hdvmconfig` command is stored in the following location:

```
installation-folder-for-Device-Manager-VDS-Provider\bin\hdvmconfig.exe
```

Table 12.2 describes the syntax and functions of the `hdvconfig` command.

Table 12.2 hdvmconfig Command Syntax and Functions

| Synopsis    | Hdvmconfig                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <p>The <code>hdvmconfig</code> command allows you to change the information used by Device Manager VDS Provider to connect to the Device Manager server. With this command, you can interactively set <code>server.ipaddress</code>, <code>server.authorization</code>, and <code>server.port</code> in the property file (<code>vds.properties</code>). To execute this command, you must have Administrator privileges. If you execute this command without Administrator privileges, an error message appears.</p> <p><b>Caution:</b> After executing the <code>hdvmconfig</code> command to modify settings in the property file, you must restart Device Manager VDS Provider.</p> <p>You need to enter the following information when requested by the <code>hdvmconfig</code> command:</p> <p><b>IP Address:</b> Enter the IP address of the Device Manager server in the dot-separated format. The specified IP address is assigned to <code>server.ipaddress</code> in the property file.</p> <p><b>User ID and Password:</b> Enter the user ID and password registered with the Device Manager server to connect to the Device Manager server.</p> <p>You can use the following characters for the user ID:</p> <pre>a-z A-Z 0-9 # + . - _ @</pre> <p><b>Note:</b> For upgrade (overwrite) installations, if you do not enter anything, the currently set user ID will be inherited.</p> <p>You can use the following characters for the password:</p> <pre>a-z A-Z 0-9 ! # \$ % &amp; ( ) * + - . = @ \ ^ _   ' ,</pre> <p>The user ID and password are encrypted by the <code>hdvmconfig</code> command and assigned to <code>server.authorization</code> in the property file.</p> <p><b>Caution:</b> Users cannot edit the data assigned to <code>server.authorization</code> because it is encrypted.</p> <p><b>Port:</b> Enter the port number of the Device Manager server. If you do not enter anything, the default 5988 is specified. The specified port number is assigned to <code>server.port</code> in the property file.</p> <p><b>Caution:</b> Specify the port number assigned to the <code>server.cim.http.port</code> in the property file (<code>server.properties</code>) used in the Device Manager server.</p> |

### 12.3.4 Device Manager VDS Provider Log Files

Problems that occur during Device Manager VDS Provider installation, uninstallation, or execution of its services are recorded in the log file.

See Table 12.3 for the log filenames, locations, and descriptions.

Table 12.3 Log Files

| Log file name and location                                                    | Description                                                                                                                 |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <i>installation-folder-for-Device-Manager-VDS-Provider\logs\hdevmcomm.log</i> | Information about communication between Device Manager VDS Provider and the Device Manager server is recorded in this file. |
| <i>installation-folder-for-Device-Manager-VDS-Provider\logs\hdevmprov.log</i> | Information about the starting and stopping of Device Manager VDS Provider is recorded in this file.                        |
| <i>Windows-system-drive:\DeviceManager 5 1 VDS</i>                            | Information about the installation execution for Device Manager VDS Provider is recorded in this file.                      |

Install.log

Windows-system-  
drive:\DeviceManager\_VDS\_  
UninstallLog.log

Information about the uninstallation execution for Device Manager VDS Provider is recorded in this file.

If a problem occurs in Device Manager VDS Provider, you can use the error information batch collection tool (`hdvmgetlogs.bat`). This tool collects the log files and property files required for error analysis from the Device Manager VDS Provider environment in a single operation. To execute this tool, you must have Administrator privileges.

`hdvmgetlogs.bat` is stored in the following location:

`installation-folder-for-Device-Manager-VDS-Provider\bin`

The format of `hdvmgetlogs.bat` is: `hdvmgetlogs.bat` (no arguments)

When you execute `hdvmgetlogs.bat`, a `resultDir` folder is created under *installation-folder-for-Device-Manager-VDS-Provider*. This folder stores the collected log files and property files.

**Caution:** If the `resultDir` folder already exists, the following confirmation message appears:

Output Directory "resultDir" already exists.  
This program will delete "resultDir" before working. continue?  
(Y)es or (N)o :

When you enter `y`, the command deletes the `resultDir` folder, and stores the acquired error information files in a new `resultDir` folder. When you enter `n`, processing is canceled.





## Acronyms and Abbreviations

|        |                                                                         |
|--------|-------------------------------------------------------------------------|
| ACL    | Access Control List                                                     |
| AMS    | Adaptable Modular Storage                                               |
| API    | application program interfaces                                          |
| CCI    | Command Control Interface                                               |
| CLI    | Command Line Interface                                                  |
| COW    | Copy on Write                                                           |
| CSR    | Certificate Signing Request                                             |
| DAMP   | Java Web Start                                                          |
| DASD   | direct access storage device                                            |
| DHCP   | Dynamic Host Configuration Protocol                                     |
| GB     | gigabyte(s)                                                             |
| GUI    | Graphical User Interface                                                |
| IETF   | Internet Engineering Task Force                                         |
| JDK    | Java Development Kit                                                    |
| JRE    | Java Runtime Environment                                                |
| JWS    | Java WE                                                                 |
| kB     | kilobyte(s)                                                             |
| LAN    | local-area network                                                      |
| LDEV   | logical device                                                          |
| LUN    | Logical unit number                                                     |
| MOF    | Managed Object Format                                                   |
| MSCS   | Microsoft Cluster Service                                               |
| NSC    | Network Storage Controller                                              |
| PKI    | Public Key Infrastructure                                               |
| SNMP   | Simple network management protocol (part of the TCP/IP protocol suite). |
| SSL    | Secure Sockets Layer                                                    |
| SVP    | Service Processor                                                       |
| TCP/IP | transmission control protocol/internet protocol                         |
| TLS    | Transport Layer Security                                                |
| USP    | Universal Storage Platform                                              |
| VDS    | Virtual Disk Service                                                    |
| WMS    | Workgroup Modular Storage                                               |

|     |                |
|-----|----------------|
| WWN | Worldwide name |
|-----|----------------|

# Index

2

23032/tcp, 215

9

9900 and 9900V

incorrect LAN configuration

illustration, 37

incorrect LAN configuration illustration, 38

A

account.lock.num, 225

authentication

using Java tool, 287

B

backing up server database

Windows, 105

C

changing server keypass

instructions, 255

changing server keystore password

instructions, 257

changing truststore password

instructions, 263

CIM properties, 354

cimom.properties file, 356

jserver.properties file, 355

server.properties file, 354

CIM/WBEM

overview, 347

CIM/WBEM feature

user permissions, 360

CIM/WBEM features

basic settings, 350

Device Manager, 349

modification of the port numbers, 352

preparations for operating, 350

CIM/WBEM security settings, 275

client properties

client.assignlun.upperlimit.enabled, 311

client.logger.trace, 309

client.message.timeout, 310

table.ldev.rowsperpage, 310

Client Properties, 309-11

cluster configuration

performing upgrade installation from version 3.5 or earlier, 164

performing upgrade installation from version 4.0 or later, 169

system requirements, 149

cluster environment

performing upgrade installation (from version 3.5 or earlier), 87

cluster environment

upgrade and re-installation, 87

- cluster server environment
  - system requirements, 149
- Cluster Server environment
  - installing in executing and standby nodes, 149
- cluster server environment (Solaris), 149
- common component
  - stopping, 207
- Common Component, 205–9
  - changing ports, 213
  - default ports, 212
  - installing and uninstalling, 205
  - integrated logging output log files, 208
  - overview, 24
  - starting, 206
  - stopping, 207
- Common Component elements
  - table, 206
- configuration definition files, 233
- configuring
  - HBase Storage Mgmt Web Service for SSL, 265–64
    - creating CSR, 267
    - disabling SSL, 271
    - enabling SSL, 269
    - self-signed certificate, 268
  - HBase Storage Mgmt Web Service for SSL
    - changing SSL port, 272
- configuring HBase Storage Mgmt Web Service for SSL
  - generating private key, 265
- configuring networks, 37
  - common security risks, 38
  - dual-homed management servers plus separate management LAN, 42
  - flat network, 43
  - overview, 37
  - separate management LAN plus firewall, 40
  - separate management LAN plus firewalled devices, 41
- contacting Hitachi Data Systems Support Center, 345
- conversion, cluster, 98
- conversion, InterBase to HiRD8, 96
- converting
  - Device Manager Server Database, 173
- copy pairs
  - requirements for, 229
- COW Snapshot, 230
- creating a keypair
  - instructions, 242
- creating CSR
  - instructions, 247

## D

- database properties, 304
  - dbm.trace.SQL, 304
- database.properties
  - dbm.startingCheck.retryCount, 304
  - dbm.startingCheck.retryPeriod, 304

- deleting
  - warning banner message, 228
- deleting keystore entry
  - instructions, 253
- deleting truststore entry
  - instructions, 261
- Device Manager
  - new functions in 5.5, 35
  - overview, 21
  - overview of software components, 22
  - related software products, 24
  - system configuration, 22
- Device Manager Server
  - converting, 173
  - Solaris upgrade installation of, 140
  - uninstalling (in Solaris), 191
- Device Manager Server database
  - converting InterBase to HiRDB, 189
  - initializing, 187
- Device Manager VDS Provider, 22
- dispatcher properties, 305-8
  - server.dispatcher.agent.priority, 307
  - server.dispatcher.daemon.pollingPeriod, 308
  - server.dispatcher.message.timeout, 307
  - server.dispatcher.traps.purgePeriod, 308
- displaying keystore contents (regular mode)
  - instructions, 251
- displaying keystore contents (verbose mode)
  - instructions, 252
- displaying truststore contents
  - instructions, 259

## E

- editing
  - warning banner message, 226
- enabling TLS/SSL
  - instructions, 245
- error information
  - hdvmgetlogs.bat, 374

## F

- firewall, working with network, 44

## G

- Glossary, acronyms and abbreviations, 375

## H

- hcmdslink, using to register, 217
- HiRD8
  - converting manually to, 189
- HiRDB scripts, 168
- host name, changing, 220

I

IETF, 239

importing signed certificate  
instructions, 249

incorrect LAN configuration  
9900 and 9900V, 37, 38

installation

Device Manager to Solaris OS, 152  
new Device Manager Server (Windows), 59  
upgrade (Windows), 66

installing

HiCommand Common Component, 205  
Linux system requirements, 121  
on executing node, 82  
on standby node, 84  
Solaris overview, 121  
Solaris system requirements, 121  
Windows, 49  
Windows overview, 49  
Windows system requirements, 49

installing VDS Provider

new installation, 366  
re-installation for correcting the same version, 368  
upgrading (installation for updating an earlier version), 367

instructions

backing up server database (Linux), 180  
backing up server database (Solaris), 179  
changing server keypass, 255  
changing server keystore password, 257  
changing truststore password, 263  
configuring HBase Storage Mgmt Web Service for SSL, 265–64  
changing SSL port, 272  
creating CSR, 267  
disabling SSL, 271  
enabling SSL, 269  
generating private key, 265  
self-signed certificate, 268

creating a keypair, 242

creating and importing signed certificate, 247–50

creating CSR, 247

deleting keystore entry, 253

deleting truststore entry, 261

displaying keystore contents (regular mode), 251

displaying keystore contents (verbose mode), 252

displaying truststore contents, 259

enabling TLS/SSL security, 245

importing signed certificate, 249

installing

Windows Device Manager Server and Common Component, 54–79

installing (Linux HiCommand Device Manager server and HiCommand Suite Common Component), 126

migrating server database Windows, 107, 182

restoring server database

Solaris, 180

restoring server database (Linux), 180

- restoring server database Windows, 106
- starting and stopping Device Manager server (Linux), 176
- starting and stopping Device Manager server (Solaris), 176
- starting and stopping the Device Manager Server
  - Windows, 102
- starting Common Component, 206
- stopping Common Component, 207
- stopping the Common Component, 207
- uninstalling (Windows HiCommand Device Manager server), 115
- uninstalling (Windows InterBase), 118
- uninstalling (Windows InterClient), 119
- verifying Linux Common Component (installation), 176
- verifying Linux Device Manager (installation), 175
- verifying Solaris Common Component (installation), 175
- verifying Solaris Device Manager installation, 175
- verifying Windows HiCommand Device Manager Server and Common Component installation, 101
- integrated logging
  - output log files, 208
- InterBase server
  - uninstalling, 118, 196
- InterClient
  - uninstalling, 119, 197

## K

- kernel parameters
  - setting, 197
  - setup needed after uninstallation of Device Manager server, 200, 203
- kernel parameters, setting, 197
- keypair, creating, 241

## L

- Linux
  - installation, 121
  - performing upgrade installation from version 4.0 or later, 144
  - Setting Kernel Parameters and Shell Restrictions, 201
  - starting and stopping Device Manager server, 177
  - system requirements, 121
  - verifying Common Component installation, 175
  - verifying Device Manager installation, 175
- logger properties, 305-7
  - logger.hicommandbase.loglevel, 306
  - logger.hicommandbase.MaxBackupIndex, 306
  - logger.hicommandbase.MaxFileSize, 306
  - logger.hicommandbase.sysloglevel, 306
  - logger.loglevel, 305
  - logger.MaxBackupIndex, 305
- LUN counts, managing, 124

## M

- Microsoft Cluster Server
  - configuring, 85
- Microsoft Cluster Server environment, 79-87
  - system requirements, 79
- Microsoft Cluster Server environment



- new installation, 82
- migrating server database
  - Windows, 107, 182
- MIME properties, 309

## N

- new functions
  - Device Manager 5.5, 35

## O

- overview
  - Common Component, 24
  - Device Manager, 21
  - Device Manager software components, 22
  - Linux Installation, 121
  - network configuration, 37
  - related software products, 24, 30
  - Solaris installation, 121
  - Solaris Installation, 121
  - Windows installation, 49

## P

- password.check.userID, 224
- password.min.length, 224
- password.min.lowercase, 224
- password.min.numeric, 224
- password.min.symbol, 224
- password.min.uppercase, 224
- port usage
  - changing Common Component, 213
- properties, Device Manager Server, 291

## Q

- QuickShadow, 229

## R

- registering
  - warning banner message, 227
- related software products
  - overview, 24, 30
- restoring server database
  - Linux, 180
  - Solaris, 180
  - Windows, 106

## S

- security counts, managing, 125
- security procedures
  - changing server keypass
    - instructions, 255
  - changing server keystore password
    - instructions, 257
  - changing truststore password
    - instructions, 263

- configuration networks, 40
- configuring HBase Storage Mgmt Web Service for SSL, 265–64
  - changing SSL port, 272
  - creating CSR, 267
  - disabling SSL, 271
  - enabling SSL, 269
  - generating private key, 265
  - self-signed certificate, 268
- configuring networks
  - dual-homed management servers plus separate management LAN, 42
  - flat network, 43
  - separate management LAN plus firewall, 40
  - separate management LAN plus firewalled devices, 41
- configuring networks (common security risks), 38
- configuring networks (dual-homed management servers plus separate management LAN), 43
- configuring networks (flat network), 44
- configuring networks (overview), 37
- configuring networks (separate management LAN plus firewall), 41
- configuring networks (separate management LAN plus firewalled devices), 42
- creating a keypair, 242
- creating and importing signed certificate
  - instructions, 247–50
- creating CSR
  - instructions, 247
- deleting keystore entry
  - instructions, 253
- deleting truststore entry
  - instructions, 261
- displaying keystore contents (regular mode)
  - instructions, 251
- displaying keystore contents (verbose mode)
  - instructions, 252
- displaying truststore contents
  - instructions, 259
- enabling TLS/SSL
  - instructions, 245
- importing signed certificate
  - instructions, 249
- security properties, 311
  - server.http.secure, 311
  - server.http.security.clientIP, 313
  - server.http.security.realm, 313
  - server.http.security.unprotected, 314
  - server.https.keystore.keypass, 314
  - server.https.keystore.passphrase, 314
  - server.https.security.keystore, 313
  - server.https.security.truststore, 315
  - server.https.truststore, 315
- security settings for user accounts, 223
- security.conf, 223
- server and common component DB
  - backing up (Sun), 179
- server database

- initializing, 113
- restoring, 106
- server properties
  - Client Properties, 309–11
  - database properties, 304
  - dispatcher properties, 305–8
  - logger properties, 305–7
  - MIME properties, 309
  - security properties, 311
  - SNMP trap properties, 311–20
  - web configuration properties, 297–304
- server security
  - important terms and concepts, 238
- server.cim.http.port, 303
- server.cim.https.support, 303
- server.configchange.autorefresh.lastrefreshed, 303
- service discovery feature, 356
  - setting up, 356
  - starting and stopping, 359
- service processor, 37
- Setting
  - Microsoft Cluster Service™, 79
- setting kernel parameter and shell restriction
  - Linux, 201
- settings
  - warning banner, 225
- ShadowImage, 229
- signed certificate
  - creating and importing
    - instructions, 247–50
- SNMP trap properties, 311–20
  - customizedsnmptrap.customizelist, 317
  - log output customization, 316
- Solaris
  - installation, 121
  - performing upgrade installation from version 3.5 or earlier, 140
  - performing upgrade installation from version 4.0 or later, 144
  - restoring server database, 180
  - restoring sever database, 180
  - starting and stopping Device Manager server, 176
  - system requirements, 121
  - uninstalling Device Manager Server cluster environment, 193
  - verifying Common Component installation, 175
  - verifying Device Manager installation, 175
- Solaris installation, 131
  - to Solaris OS, 131
- starting
  - VDS provider, 369
- stopping
  - VDS service provider, 370
- Storage Navigator Modular (for Web)
  - linking with, 323
- suitesrvctl, 103
- Sun cluster

- cluster resource setup, 162
- configuring, 172
- Sun cluster scripts, 156
- SVP, 37

## T

- troubleshooting
  - contacting Hitachi Data Systems, 345
  - HBase Storage Mgmt Common Service, 101
  - HBase Storage Mgmt Common Service, 101
  - HBase Storage Mgmt Web Service, 101
  - problems and solutions, 335
  - thread dump, 345
  - using TIA, 343
- troubleshooting Windows installation
  - HiCommand server does not start, 101
  - HiCommand server not in Services panel, 101
  - SSOS or CWS not in Services panel, 101
- TrueCopy, 229

## U

- uninstalling, 114, 191
  - HiCommand Common Component, 205
  - Windows HiCommand Device Manager Server, 114
  - Windows HiCommand Device Manager server (cluster environment), 116
  - Windows InterBase, 118
  - Windows InterClient, 119
- Universal Replicator, 229
- upgrading considerations, Solaris, 137
- upgrading Device Manager Server (Windows), 68, 74

## V

- VDS provider
  - starting, 369
- VDS Provider
  - changing settings, 372
  - functions, 363
  - installing, 365
  - log files, 373
  - overview, 363
  - property files, 370
  - uninstalling, 368
- VDS Provider property files
  - logger.properties, 371
  - vds.properties, 371
- VDS service provider
  - stopping, 370
- verifying
  - Linux Common Component installation, 175
  - Solaris Common Component installation, 175
  - Solaris Device Manager installation, 175
- VERITAS cluster server
  - configuring, 172
- VERITAS Cluster Server

- cluster resource setup, 159
- VERITAS cluster server scripts, 155

## W

### warning banner

- deleting message, 228
- editing message, 226
- registering message, 227
- settings, 225

### web configuration properties, 297–304

- server.base.home, 302
- server.base.initialsynchro, 302
- server.cim.support, 302
- server.cim.support.protocol, 303
- server.horcmconfigfile.hostname, 302
- server.http.cache.maxFileSize, 301
- server.http.cache.size, 300
- server.http.connection.bufSize, 298
- server.http.connection.priority, 298
- server.http.default, 297
- server.http.entity.maxLength, 300
- server.http.fileTypes.noLog, 301
- server.http.headers.maxLength, 300
- server.http.headers.maxNumber, 299
- server.http.host, 297
- server.http.log.reverseDNS, 300
- server.http.mode, 301
- server.http.port, 297
- server.http.request.timeout, 298
- server.http.socket.backlog, 298
- server.http.socket.linger, 299
- server.http.socket.maxThreads, 299
- server.http.socket.noDelay, 299
- server.https.port, 297
- server.installTime, 301

### Windows

#### installing

### Windows

#### installing

- Device Manager Server and Common Component, 54–79
- performing re-installation, 72
- performing upgrade installation (from 4.0 or later), 72
- performing upgrade installation (from version 3.5 or earlier), 66
- system requirements, 49

### Windows

- Verifying and Troubleshooting Installation of HiCommand Device Manager Server and Common Component, 100

### Windows

- starting and stopping the Device Manager Server, 102

### Windows

- restoring server database, 106

### Windows

- migrating server database, 107

### Windows

- uninstalling HiCommand Device Manager Server, 114
- Windows
  - uninstalling Windows components, 116
- Windows
  - uninstalling HiCommand Device Manager server (cluster environment), 116
- Windows
  - migrating server database, 182
- Windows installation
  - troubleshooting
    - HiCommand server does not start, 101
    - SSOS or CWS not in Services panel, 101
  - troubleshooting (HiCommand server not in Services panel), 101