HITACHI
Inspire the Next

Hitachi Unified Storage File Module

Antivirus Administration Guide

Release 12.1

Hitachi Data Systems

MK-92USF010-03

Hitachi Data Systems products and services can be ordered only under the terms and conditions of Hitachi Data Systems' applicable agreements. The use of Hitachi Data Systems products is governed by the terms of your agreements with Hitachi Data Systems.

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

Archivas, Dynamic Provisioning, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, OS/390, RS6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, zSeries, z/VM, z/VSE are registered trademarks and DS6000, MVS, and z10 are trademarks of International Business Machines Corporation.

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

Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Some parts of ADC use open source code from Network Appliance, Inc. and Traakan, Inc.

Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are copyright 2001-2009 Robert A. Van Engelen, Genivia Inc. All rights reserved. The software in this product was in part provided by Genivia Inc. and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

The product described in this guide may be protected by one or more U.S. patents, foreign patents, or pending applications.

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.

Contents

Preface

In PDF format, this guide describes the supported antivirus engines, provides information about how to enable them, and how to configure the system to use them.

Document revision level

Revision	Date	Description
MK-92USF010-00	July 2012	First publication
MK-92USF010-01	September 2012	Revision 1, replaces and supercedes MK-92USF010-00
MK-92USF010-02	August 2013	Revision 2, replaces and supercedes MK-92USF010-01
MK-92USF010-03	September 2014	Revision 3, replaces and supercedes MK-92USF010-02

Contacting Hitachi Data Systems

2845 Lafayette Street
Santa Clara, California 95050-2627
U.S.A.
https://portal.hds.com
North America: 1-800-446-0744

Related Documentation

Release Notes provide the most up-to-date information about the system, including new feature summaries, upgrade instructions, and fixed and known defects.

Administration Guides

- *System Access Guide* (MK-92USF002)—In PDF format, this guide explains how to log in to the system, provides information about accessing the NAS server/cluster CLI and the SMU CLI, and provides information about the documentation, help, and search capabilities available in the system.
- *Server and Cluster Administration Guide* (MK-92USF007)—In PDF format, this guide provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces,

upgrading firmware, monitoring servers and clusters, the backing up and restoring configurations.

- *Storage System User Administration Guide* (MK-92USF011)—In PDF format, this guide explains user management, including the different types of system administrator, their roles, and how to create and manage these users.
- *Network Administration Guide* (MK-92USF003)—In PDF format, this guide provides information about the server's network usage, and explains how to configure network interfaces, IP addressing, name and directory services.
- *File Services Administration Guide* (MK-92USF004)—In PDF format, this guide explains about file system formats, and provides information about creating and managing file systems, and enabling and configuring file services (file service protocols).
- *Data Migrator Administration Guide* (MK-92USF005)—In PDF format, this guide provides information about the Data Migrator feature, including how to set up migration policies and schedules.
- *Storage Subsystem Administration Guide* (MK-92USF006)—In PDF format, this guide provides information about managing the supported storage subsystems (RAID arrays) attached to the server/cluster. Includes information about tiered storage, storage pools, system drives (SDs), SD groups, and other storage device related configuration and management features and functions.
- *Snapshot Administration Guide* (MK-92USF008)—In PDF format, this guide provides information about configuring the server to take and manage snapshots.
- *Replication and Disaster Recovery Administration Guide* (MK-92USF009)—In PDF format, this guide provides information about replicating data using file-based replication and object-based replication, provides information on setting up replication policies and schedules, and using replication features for disaster recovery purposes.
- *Antivirus Administration Guide* (MK-92USF010)—In PDF format, this guide describes the supported antivirus engines, provides information about how to enable them, and how to configure the system to use them.
- *Backup Administration Guide* (MK-92USF012)—In PDF format, this guide provides information about configuring the server to work with NDMP, and making and managing NDMP backups. Also includes information about Hitachi NAS Synchronous Image Backup.
- *Command Line Reference*—Opens in a browser, and describes the commands used to administer the system.

Note: For a complete list of Hitachi NAS open source software copyrights and licenses, see the *System Access Guide*.

Hardware References

- *Hitachi Unified Storage File Module 3080 3090 G2 Hardware Reference* (MK-92USF001)—Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- *Hitachi Unified Storage File Module 4000 Hardware Reference* (MK-92HNAS030) —Provides an overview of the Hitachi Unified Storage File Module 4000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.

Best Practices

- *Hitachi USP-V/VSP Best Practice Guide for HNAS Solutions* (MK-92HNAS025)—The HNAS practices outlined in this document describe how to configure the HNAS system to achieve the best results.
- *Hitachi Unified Storage VM Best Practices Guide for HNAS Solutions* (MK-92HNAS026)—The HNAS system is capable of heavily driving a storage array and disks. The HNAS practices outlined in this document describe how to configure the HNAS system to achieve the best results.
- *Hitachi NAS Platform Best Practices Guide for NFS with VMware vSphere* (MK-92HNAS028)—This document covers VMware best practices specific to HDS HNAS storage.
- *Hitachi NAS Platform Deduplication Best Practice* (MK-92HNAS031) —This document provides best practices and guidelines for using HNAS Deduplication.
- *Hitachi NAS Platform Best Practices for Tiered File Systems* (MK-92HNAS038) —This document describes the Hitachi NAS Platform feature that automatically and intelligently separates data and metadata onto different Tiers of storage called Tiered File Systems (TFS).
- *Hitachi NAS Platform Data Migrator to Cloud Best Practices Guide* (MK-92HNAS045)—Data Migrator to Cloud allows files hosted on the HNAS server to be transparently migrated to cloud storage, providing the benefits associated with both local and cloud storage.
- *Brocade VDX 6730 Switch Configuration for use in an HNAS Cluster Configuration Guide* (MK-92HNAS046)—This document describes how to configure a Brocade VDX 6730 switch for use as an ISL (inter-switch link) or an ICC (inter-cluster communication) switch.
- *Best Practices for Hitachi NAS Universal Migrator* (MK-92HNAS047)—The Hitachi NAS Universal Migrator (UM) feature provides customers with a convenient and minimally disruptive method to migrate from their existing NAS system to the Hitachi NAS Platform. The practices and recommendations outlined in this document describe how to best use this feature.
- *Hitachi NAS Platform Storage Pool and HDP Best Practices* —This document details the best practices for configuring and using HNAS storage pools, related features, and Hitachi Dynamic Provisioning (HDP).

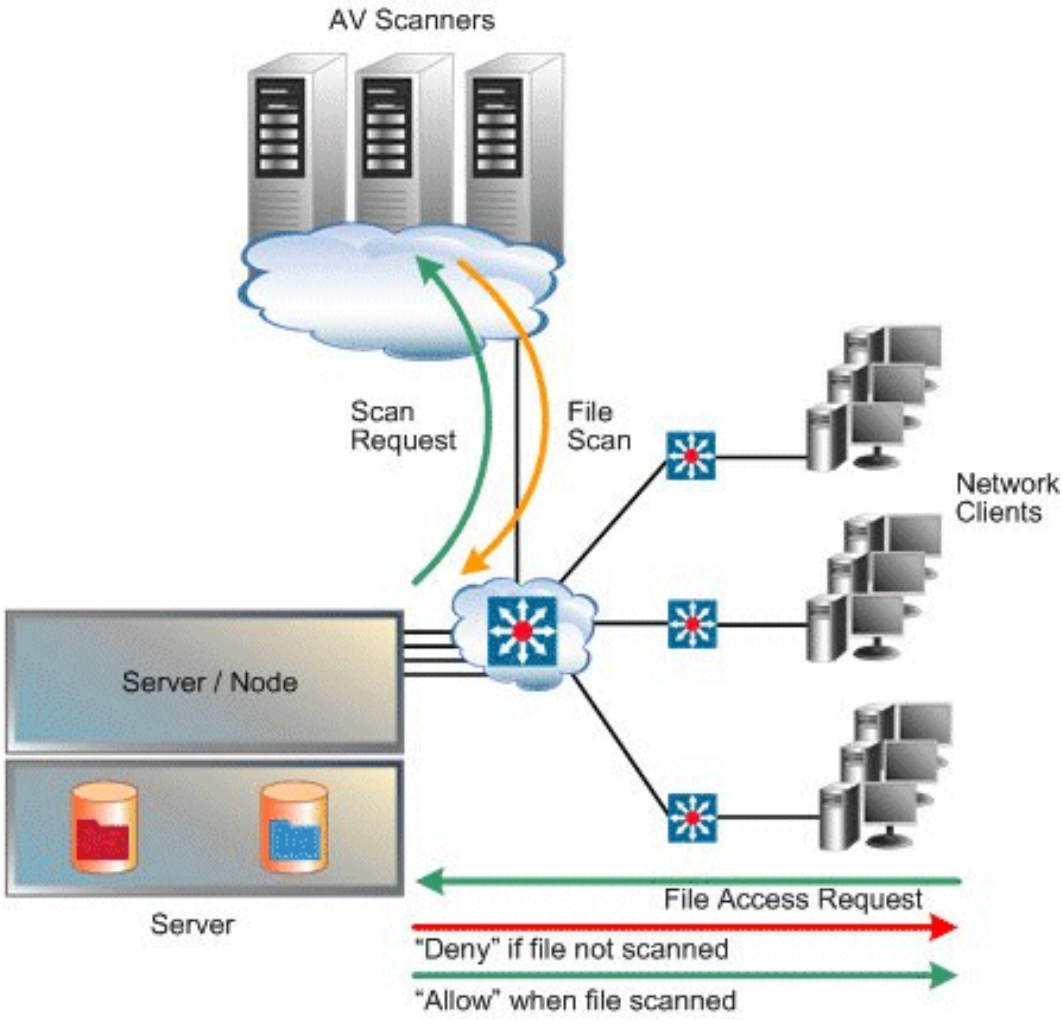
1

About virus scanning

The storage server architecture reduces the effect of a virus because the file system is hardware-based. This prevents viruses from attaching themselves to (or deleting) system files required for server operation. However, viruses can still propagate and infect user data files that are stored on the server. Therefore, Hitachi Data Systems works with industry leading antivirus (AV) software vendors to ensure that the server integrates into an organization's existing AV solutions and without requiring special installations of AV software and servers. To reduce the effect that a virus may have on user data, Hitachi Data Systems Support Center recommends that AV be configured for the server and that AV software run on all user workstations.

Virus scanning overview

The server itself does not perform any scanning of the files, but rather provides a connection with configured Virus Scan Engines on the network:



You can configure multiple Virus Scan Engines to enhance both the performance and to maintain high-availability of the server. If a Virus Scan Engine fails during a virus scan, the storage server automatically redirects the scan to another Virus Scan Engine.

The server maintains a list of file types, the Inclusion List, that allows the administrator to control which files are scanned (for example, .exe, .dll, .doc, and so forth). The default Inclusion List includes most file types commonly affected by viruses.

Caution: When virus scanning is enabled, the server must receive notification from a Virus Scan Engine that a file is clean before allowing access to the file. As a result, if virus scanning is enabled and there are no Virus Scan Engines available to service the virus scans, CIFS clients may experience a temporary loss of data access. To ensure maximum accessibility of data, configure multiple Virus Scan Engines to service each EVS on which virus scanning has been enabled.

If virus scanning is temporarily disabled, files continue to be marked as needing to be scanned. In this way, if virus scanning is re-enabled, files that were changed are re-scanned the next time they are accessed by a CIFS client.

Virus Scanning statistics for the storage server (in 10-second time slices) are available for activity since the previous reboot or since the point when statistics were last reset.

Note: When a virus is detected, a severe event is placed in the Event Log, identifying the path of the infected file and the IP address of the infected machine. For information on accessing the event log, see the *Server and Cluster Administration Guide*.

You can also set a list of file types on a file system that will be excluded from being sent for scanning by antivirus servers. With an exclusion list you can scan all files except those with certain file extensions, for example, those containing application data. This helps reduce the load on the virus scanning engines and network.

As with the inclusion list, the exclusion list will support wildcarding. The exclusion list is configurable using the command line interface.

Using the Internet Content Adaption Protocol (ICAP)

The Internet Content Adaption Protocol (ICAP) is an open standard being adopted to connect devices to enterprise-level virus scan engines. ICAP is becoming the preferred means of virus scanning over the previous RPC-based mechanism of virus scanning.

ICAP provides simple object-based content vectoring for HTTP services. ICAP is a protocol for executing a remote procedure call on HTTP messages. It allows ICAP clients to pass HTTP messages to ICAP servers for transformations or other processing (adaptation). The server executes its transformation service on messages and sends back responses to the client, usually with modified messages. Typically, the adapted messages are either HTTP requests or HTTP responses.

ICAP is primarily designed to facilitate the deployment of various value-added services to web serving systems. Inbound and outbound HTTP traffic can be

modified by diverting requests or responses through an “ICAP Server”. This server performs content adaptation, such as ad insertion or virus scanning. ICAP is also used in non-web serving environments, such as NAS systems in which client/server protocols have similar requirements for content adaptation. In NAS platforms, ICAP virus scanning cleans file before they are sent. A client requests files, and the NAS platform delegates the task of ensuring these files are clean to external systems, called “scan engines”, before sending them to the client.

The ICAP feature does not require installation. It can be configured using the CLI or SMU. There are no special prerequisites in terms of hardware platform or licenses (ICAP is not a licensed feature). Virus scanning may impact performance when enabled as it adds an overhead when reading files as they are scanned. The performance impact will depend on the number of virus scan engines connected to the system and the dynamic nature of the data on the NAS system.

All virus scan related settings apply at the per-EVS level.

Configuring virus scan engines

You should configure multiple virus scan engines to enhance performance and high-availability of the server.

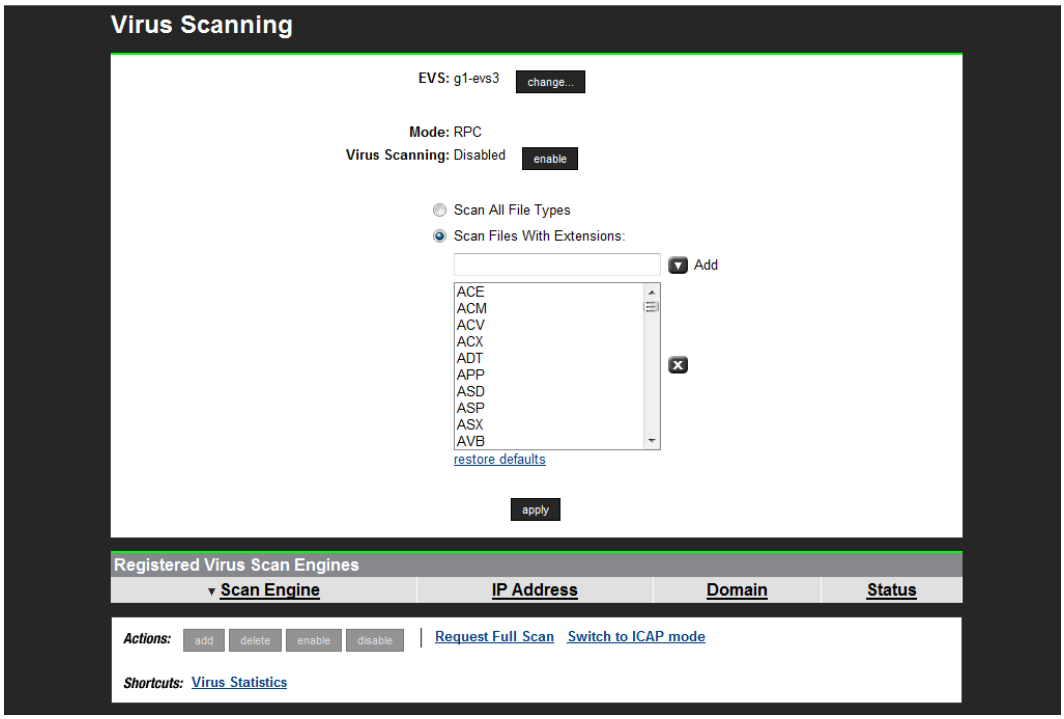
You may select between the RPC protocol or ICAP when setting up new virus scan engines.

After installation and configuration has been completed, the virus scan engine will automatically self-register with the server.

Enabling virus scanning on the storage server

Procedure

1. Navigate to **Home > Data Protection > Virus Scanning** to display the **Virus Scanning** page.



Field/Item	Description
EVS	Displays the EVS to which this page applies. Click **change** to select a different EVS.
Mode	Indicates the virus scan mode.
Virus Scanning	Indicates whether virus scanning is enabled or disabled for the selected EVS. Click **enable** to enable virus scanning. Virus scanning can be suspended at any time by selecting the **disable** button. If virus scanning services are resumed later, any file that has changed while virus scanning services were disabled, will be scanned the next time they are accessed by a CIFS client. **Tip:** Virus scanning can be disabled on individual CIFS shares by clearing the **Enable Virus Scanning** check box in the **Add Shares** page (**File Services > CIFS Shares > Add Share**) or the **CIFS Share Details** page (**File Services > CIFS Shares > CIFS Share Details**). **Note:** For virus scanning to be enabled, it is important that at least one virus scan engine is listed in the **Registered Virus Scan Engines** table on this page.

Field/Item	Description
Scan All File Types	Scans all file types, regardless of those defined in the **File type to scan** list.
Scan Files With Extension	Scans specific file types, and ensure that the list of file types contains the appropriate file extensions. The default list includes most files commonly affected by viruses. To add a file type to scan, enter the file extension in the field, and click **Add**. To delete a file type from the list, select the file type, and click **X**. To revert to the original list of files to scan, select **restore defaults**. **Note:** When you choose to limit the scan to specific file types, only the file types you include in the list are scanned; file types not listed are not scanned.
apply	Saves any changes.
Registered Virus Scan Engines	Lists the virus scan engines configured for the current EVS.
Actions	• **add** opens the Add Scan Engine page. • **delete** deletes the selected virus scan engine. • **enable** enables the selected virus scan engine. • **disable** disables the selected virus scan engine.
Request Full Scan	Scans every file whether or not it has been scanned since it was last accessed.
Switch to ICAP mode/ **Switch to RPC mode**	Changes the virus scan mode.

2. Select the **Virtual Server (EVS)** on which to enable virus scanning.

Caution: It is important that at least one virus scan engine is listed in the Registered Virus Scanners table. The account used to start the scanning services on the virus scan engine must be added to the server's Backup Operators Local Group. If the account used to start the antivirus service is not a member of the Backup Operators Local Group, the antivirus engine will not be registered and will not be displayed on the **Virus Scanning** page of Web Manager. If you try to enable virus scanning when no virus scanners have been registered, the SMU restricts the action; virus scanning cannot be enabled when there are no registered virus scanners.

3. Click **enable** next to the Enable Virus Scanning field to enable scanning.

   Virus scanning can be disabled on individual CIFS shares by unchecking the **Enable Virus Scanning** box in the **Add Shares** page (**File Services > CIFS Shares > Add Share**).
4. Optionally, modify the list of files to be scanned:

- To scan all file types regardless of those in the list, select **Scan All File Types**. It is advisable to select this option while compiling your list of file types to scan.
- To add a file type to scan, click the **Scan Files With Extensions** radio button, enter the file extension in the field below it, then click **Add**.
- To delete a file type, select it from the list, and click the **X**.
- To revert back to the original default list of files types to scan, click **restore defaults**.

Caution: The default list of file extensions contains the most commonly used file types. Contact your antivirus software vendor for an up-to-date list of file types that should be included for scanning, and to modify the your file extension list accordingly. It is your responsibility to choose the file types you include for scanning. Based on your needs, the antivirus software used, and the recommendations of the antivirus software manufacturer, choose the file types you want to include in the antivirus scanning; *types not listed will not be scanned*.

The default file extension list is as follows:

```
ACE, ACM, ACV, ACX, ADT, APP, ASD, ASP, ASX, AVB, AX, BAT,
BO, BIN, BTM, CDR, CFM, CHM, CLA, CLASS, CMD, CNV, COM, CPL,
CPT, CPY, CSC, CSH, CSS, DAT, DEV, DL, DLL, DOC, DOT, DVB,
DRV, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTT,
HTW, HTX, IM, INF, INI, JS, JSE, JTD, LIB, LGP, LNK, MB, MDB,
MHT, MHTM, MHTML, MOD, MPD, MPP, MPT, MRC, MS, MSG, MSO, MP,
NWS, OBD, OBT, OBJ, OBZ, OCX, OFT, OLB, OLE, OTM, OV, PCI,
PDB, PDF, PDR, PHP, PIF, PL, PLG, PM, PNF, PNP, POT, PP, PPA,
PPS, PPT, PRC, PWZ, QLB, QPW, REG, RTF, SBF, SCR, SCT, SH,
SHB, SHS, SHT, SHTML, SHW, SIS, SMM, SWF, SYS, TD0, TLB, TSK,
TSP, TT6, VBA, VBE, VBS, VBX, VOM, VS?, VSD, VSS, VST, VWP,
VXD, VXE, WBT, WBK, WIZ, WK?, WML, WPC, WPD, WS?, WSC, WSF,
WSH, XL?, XML, XTP, 386
```

5. If a virus scanner has been disabled for some reason, you can re-enable its usage by filling the check box next to the name of the disabled virus scanner and clicking the **enable** button in the **Actions** area.
6. Verify your settings, and click **apply** to save.

Related task

[Enabling an exclusion list on page 17](#).

Forcing files to be rescanned

With the appearance of a new virus and release of antivirus software updates, it is important to rescan all files, including those that have not changed since the last time they were scanned.

Procedure

1. Navigate to **Home > Data Protection > Virus Scanning** to display the **Virus Scanning** page.
2. Click the **Request Full Scan** link.

   This marks every file as unscanned, so the file will be scanned the next time it is accessed.

Enabling an exclusion list

You can enable an exclusion list using CLI commands.

Use this procedure to enable an exclusion list of file types that will be excluded from scanning by antivirus servers.

Prerequisites

Management of an exclusion list is on a per-EVS basis.

Procedure

1. Add file types to the exclusion list by using **virussscan-exclusion-list-add** CLI command.

   ```
   virussscan-exclusion-list-add BAT,COM,DOC,EXE,PPT
   ```

   There must be no whitespace between consecutive types. 250 entries can be added to the exclusion list.
2. Enable the exclusion list by using the **virussscan-exclusion-list-enable** command.

   ```
   virussscan-exclusion-list-enable
   ```

   File types can also be removed, and the list can be disabled and cleared. See the man pages for:
   - **virussscan-exclusion-list-remove**
   - **virussscan-exclusion-list-disable**
   - **virussscan-exclusion-list-clear**

Related task

Enabling virus scanning on the storage server on page 13.

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

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

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-92USF010-03