
Hitachi Vantara - Hitachi Remote Ops Monitor Agent Installation Guide

Copyright (c) 2001, 2020 - Hitachi Vantara. All rights reserved.

Last Updated - November 2, 2020 (version 8.8)

Foreword

Note: The name 'Hi-Track' has been renamed to 'Hitachi Remote Ops'.

This document describes the procedures for installing, configuring, and running the Hitachi Vantara 'Hitachi Remote Ops Monitor Agent' program. Configuration of the Hitachi Remote Ops Monitor Agent requires the correct setting of the 'Hitachi Remote Ops Site ID' or else the function won't work properly. If not already known, obtain the Hitachi Remote Ops site ID setting from the Hitachi Vantara service/support representative.

The Hitachi Remote Ops Monitor Agent supports the following products:

- Disk Storage
 - Hitachi VSP F/G 900/700/370/350/130 Storage
 - Hitachi VSP E990 Storage
 - Hitachi HUS Storage
 - Hitachi AMS2000 Storage
 - * Note - the Hitachi VSP 5x00, VSP F/G1x00, VSP, and HUS VM devices may be configured into the Hitachi Remote Ops Monitor Agent to be monitored only to provide the status of any uncompleted SIMs. This detected condition doesn't transport the status to the Hitachi Vantara Hitachi Remote Ops Center through the agent and this level of monitoring doesn't obviate the need for the Hitachi Remote Ops SVP Agent transporting to the Hitachi Vantara Hitachi Remote Ops Center.
- Compute Servers
 - Hitachi Compute Blade Server CB 2500
 - Hitachi Compute Blade Server CB 500
 - Hitachi Compute Blade Server models CB 2000, 320, IOEU
 - Hitachi Compute Rack Server CR 2xM (CR2x0H/S)
 - Quanta T41S, D51B
 - Hitachi Advanced Server DS120/220/225 and 240
 - Hitachi Advanced Server DS7000
 - Hitachi Advanced Server 8x0
- File/Content/NAS
 - Hitachi Content Platform (HCP), HCP S Series Node (HCP-S), Hitachi Content Platform Anywhere (HCP-AW),



- Hitachi Content Platform Cloud Scale (HCP-CS)
- Hitachi High Performance NAS (HNAS)
- Hitachi Data Ingestor (HDI)
- Hitachi Ops Center Protector (HDID)
- Hitachi Content Intelligence (HCI)
- Switches/Directors
 - Brocade
 - Cisco
- Software
 - Hitachi UCP Advisor
 - Hitachi UCP Director
 - Hitachi Ops Center Automator (HAD)
- Other
 - Hitachi Protection Platform (HPP)

The Hitachi Remote Ops Monitor Agent supports being installed on the following platforms (64 bit versions only):

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows 10
- Windows 8.1
- Windows 7
- RedHat Linux x86 64 bit (version 6 or higher)
- VMWare with one of the above operating systems

The Hitachi Remote Ops Monitor Agent is available on CD and is orderable as part number IP0826-1 and may be available via the Support website. It is also available internally to Hitachi Vantara via the Hitachi Remote Ops website.

The normal distribution of the Hitachi Remote Ops Monitor Agent (IP0826-1) includes the JRE (Java Runtime Environment) necessary to run the Hitachi Remote Ops Monitor Agent application. Since this JRE is installed in a subdirectory of the Hitachi Remote Ops Monitor Agent installation directory, there is no dependency or conflict with any existing JRE that might be installed on the host platform. This distribution is to be used in locations that have no issue with export/import of the JRE from Hitachi Vantara based on export/import regulations of the specific locale and the USA.

Prior to installing the Hitachi Remote Ops Monitor Agent application, it is recommended to review the [Prerequisites section](#) and the appropriate customer preferences and network configuration noted for configuring the Hitachi Remote Ops Monitor Agent instance.



To perform this installation, follow the steps in the [Hitachi Remote Ops Monitor Agent Installation Instructions](#) section.

NOTE: These instructions apply to version 8.8 of the Hitachi Remote Ops Monitor Agent.

Functional Overview

Purpose

The Hitachi Remote Ops system provides a means of collecting maintenance information from the systems being monitored and transferring that information to a centralized location at Hitachi Vantara where the data is automatically analyzed and a service case with subsequent notification created if warranted. This benefits both the customer and Hitachi Vantara by permitting Hitachi Vantara service personnel to be notified of issues on the monitored devices immediately and pro-actively and enables the issues to be resolved faster and mitigated before they become more severe issues.

Description

The Hitachi Remote Ops Monitor Agent application is a Java application that runs on a customer supplied host platform (Windows, Linux, or virtual instance of one of these operating systems). The application monitors the devices on the customer's network that it's configured to monitor and will report the status of the device to the Hitachi Remote Ops Center at Hitachi Vantara by an HTTPS or FTP session (customer preference although HTTPS is recommended) through the public internet. The data reflecting the status is sent to the Hitachi Remote Ops Center immediately if a potential error condition is detected and the status and configuration information (microcode version, type of HDDs installed, etc.) will be sent on a daily basis even if no error condition exists.

The Hitachi Remote Ops Monitor Agent has a function that permits Hitachi Vantara support specialists to easily, quickly, and securely acquire an extended dump/log from certain devices if enabled. This permits a faster and higher level of support for those situations that require extended analysis.

The Hitachi Remote Ops Monitor Agent has a web browser interface to configure the application and to provide a mechanism for displaying the status of each monitored device by the application.

The Hitachi Remote Ops Monitor Agent includes the option to send email notifications of detected errors to a user-defined list of email locations as well as the option to send SNMP traps to a customer monitoring system. These options are for the use of the customer if the customer desires to use these features.

Normally only a single instance of Hitachi Remote Ops Monitor Agent will be installed and running at a site. This single instance will monitor all devices at the site and possibly devices at remote sites as well depending on the customer's network and device configurations. If a new device is being installed at the customer site and there is already an instance of Hitachi Remote Ops Monitor Agent installed and running at the site monitoring other devices, typically the existing Hitachi Remote Ops Monitor Agent instance would simply have the new device added to be monitored by it (a very quick and easy step) rather than installing a new instance of the Hitachi Remote Ops Monitor Agent application. A variant of this would be having a backup mode instance of Hitachi Remote Ops Monitor Agent running at the site if desired. Refer to references in this guide for the backup mode.



Permitted Usage

The Hitachi Remote Ops Monitor Agent is a service tool owned by Hitachi Vantara that is permitted to be used only with products under a current maintenance agreement with Hitachi Vantara or a Hitachi Vantara authorized service partner. The Hitachi Remote Ops Monitor Agent shall not be used without a valid maintenance agreement. If there are no products at the customer site under a maintenance agreement with Hitachi Vantara or a Hitachi Vantara authorized service partner then the application shall be de-installed by the customer or a service person. If a subset of the monitored devices are under a maintenance agreement but some are not then the ones that are not shall be removed from monitoring via the Hitachi Remote Ops Monitor Agent user interface by the customer or a service person.

Security

The following describes some key points concerning security with the Hitachi Remote Ops Monitor Agent system.

- The Hitachi Remote Ops Monitor Agent may be configured to communicate with the Hitachi Remote Ops Center via either HTTPS, FTP standard, or FTP-SSL over the public internet. The preferred transport method to use is HTTPS. The support of the FTP protocols will be phased out soon so be certain to configure only HTTPS.
- The Hitachi Remote Ops Monitor Agent only originates transports in an outbound direction (from the customer network to the Hitachi Vantara); no inbound access is required. The transport traffic must all go via the customer firewall which allows the customer to place controls, limitations, and monitors at their firewall level. This includes limiting the destination locations to strictly the ones that Hitachi Remote Ops needs to connect to and limiting the types of communications to only HTTPS/FTP/FTP-SSL originating on the inside of their firewall. The transferred data is encrypted when HTTPS or FTP-SSL is used.
- The data the Hitachi Remote Ops Monitor Agent sends to the Hitachi Remote Ops Monitor Center is maintenance related information that's not considered sensitive data by most customers. The data pertains to the current health of the device (power supplies, disk drives, fans, etc.) and some basic configuration data such as microcode/firmware levels, capacity, types of HDDs, etc. of the devices monitored.
- The Hitachi Remote Ops Monitor Agent system never accesses or transports customer data stored on the monitored devices.
- The Hitachi Remote Ops Monitor Agent has been audited by an independent security testing firm, ICSA Labs, and tested to not expose the customer's network to any threats. The security audit report may be downloaded from the Hitachi Vantara website as well as the ICSA Labs website.
- Hitachi Remote Ops Monitor Agent may be optionally configured to use Active Directory for user logon credentials rather than the default local credentials.
- The Hitachi Remote Ops Monitor Agent may be optionally configured to use HTTPS (secure) browser accesses to it for the user interface rather than the default HTTP although this typically isn't needed since this access is contained within the customer's network.

Prerequisites

- **Host Platform**

The customer must supply a Windows or Linux x86 host platform on which to run the Hitachi Remote Ops Monitor Agent. The Monitor Agent has been tested to run on VMWare running an instance of one of the stated operating systems. The recommended configuration of the platform for the Monitor Agent is generally the same as the recommended platform configuration as determined by the provider of the particular operating system and can be



found on the websites of those providers. This platform needs to run 24/7 in order to properly perform the Hitachi Remote Ops function. It is possible that the platform may be used for running other applications as long as the Hitachi Remote Ops Monitor Agent is running concurrently.

- **Network - Between the Hitachi Remote Ops Monitor Agent host platform and the monitored devices**

There must be TCP/IP network connectivity to the monitored device by the Hitachi Remote Ops Monitor Agent host platform. The ports and protocols Hitachi Remote Ops Monitor Agent uses to monitor the device depends on the particular device type. The following table indicates which default ports and protocols must be accessible on the device from the Hitachi Remote Ops Monitor Agent platform. These ports must be open between the Hitachi Remote Ops Monitor Agent host platform and the monitored device

Device Type	Port (Protocol)
VSP F/G 900/700/370/350/130	443 (HTTPS)
VSP E990	443 (HTTPS)
HUS, AMS, WMS, SMS	2000 (*See note 1), 80 (HTTP), 28355 (If using SSL access)
HCP	161 (SNMP) (*See note 2), 9090 (HTTP)
HCP S Series (HCP-S)	9090 (HTTPS)
HCP-AW	161 (SNMP) (*See note 2)
HCP-CS	8000 (HTTPS), 9099 (HTTPS)
Hitachi Content Intelligence (HCI)	8000 (HTTPS)
Hitachi Data Ingestor (HDI)	443 (HTTPS)
Hitachi Ops Center Protector (HDID)	443 (HTTPS)
HNAS	22 (SMU access via SSH)
Hitachi Protection Platform (HPP)	22 (SFTP)



Compute Blade Server CB 2500	443 (HTTPS), 23 (Telnet)
Compute Blade Server CB 500	443 (HTTPS), 23 (Telnet)
Compute Blade Server 2000, 320, IOEU	161 (SNMP) (*See note 2), 21 (FTP), 23 (Telnet)
Compute Rack Server CR xM (CR 2x0H/S)	443 (HTTPS)
Quanta Server, Hitachi Advanced Server DS120/220/225, 240	161 (SNMP) (*See note 2)
Hitachi Advanced Server DS7000	443 (HTTPS), 623 UDP (IPMI)
Hitachi Advanced Server 8x0	443 (HTTPS)
UCP Advisor	443 (HTTPS/JSON)
UCP Director	443 (HTTPS/JSON)
Hitachi Ops Center Automator (HAD)	443 (HTTPS/JSON)
Brocade Switch/Director	161 (SNMP) (*See note 2), 22 (SSH) on both Brocade device and Hitachi Remote Ops Monitor Agent platform
Cisco Switch/Director	161 (SNMP) (*See note 2), 22 (SSH) on Cisco device

- **Note 1** - It is possible that the HUS/AMS device's default monitoring port, **port 2000**, was configured to use a different port. If so, the Hitachi Remote Ops Monitor Agent must be configured to use the port configured in the device if using a different port than the default, 2000.

Note 2 - If a device is being monitored via the SNMP protocol the device must be configured to allow SNMP Get functions from the Hitachi Remote Ops Monitor Agent. Refer to the documentation and configuration procedures for the particular device to ensure the SNMP facility is configured properly on the device. The community string (for SNMP v1/2) or User/Password (for SNMP v3) in the Hitachi Remote Ops Monitor Agent will need to exactly match



(including case sensitivity) the equivalent setup in the device. The SNMP v1/2 community string is "public" by default. The Cisco device and some other devices use SNMP v3. The HCP-AW/HCP devices are configurable for either SNMP v1/2 or SNMP v3. Some devices will only allow SNMP access from a list of pre-defined IP addresses in its user interface. For these devices be sure to include the IP address of the host platform running the Hitachi Remote Ops Monitor Agent application. Note that the Hitachi Remote Ops Monitor Agent doesn't receive SNMP traps from the device, it only performs SNMP Gets, so it's not necessary to configure the device to send SNMP traps to the Hitachi Remote Ops Monitor Agent.

- **Network - Between the Hitachi Remote Ops Monitor Agent host platform and the internet**
 - **HTTPS:** If using HTTPS, the recommended protocol, as the transport from the Hitachi Remote Ops Monitor Agent to the Hitachi Vantara Hitachi Remote Ops Center, there must be connectivity to the standard HTTPS **port 443**. The customer may use an HTTPS proxy if desired in which case the customer must supply the parameters to use with their particular proxy server as required.
 - **FTP:** If using FTP as the transport from the Hitachi Remote Ops Monitor Agent to the Hitachi Vantara Hitachi Remote Ops Center, there must be FTP Put/Append capability for passive FTP transfers using the standard FTP ports. The ports used are **port 21** for non-SSL, **port 990** for SSL, and **ports 50000-50024** for the passive data connection. The FTP Puts and Appends are from the Hitachi Remote Ops Monitor Agent host platform to the public internet. The customer's firewall must be configured to allow this type of protocol connection through the specified port range by the customer's network administrator if it isn't currently enabled. The FTP Put/Append needs to be enabled only in an outbound direction originating within the customer's network. The customer may use an FTP proxy if desired in which case the customer must supply the parameters to use with their particular proxy server if required.

Maximum Number of Devices Supported

The maximum number of devices that can be supported by the particular Hitachi Remote Ops Monitor Agent application has no artificial limit but will be limited practically based on the following variables -

- Latency in the customer network from the Hitachi Remote Ops Monitor Agent to the device - i.e. a Hitachi Remote Ops Monitor Agent located on one continent monitoring a device on another continent through a WAN will likely have more inherent delays in acquiring data than a device on the same subnet as the application and located close to each other.
- Speed and capacity of the customer's network.
- Capability and loading of the platform hosting the Hitachi Remote Ops Monitor Agent.
- Types of devices being monitored.
- Scan (poll) interval timing. This is the time interval between each contact with a particular device by the Hitachi Remote Ops Monitor Agent.

The actual loading of the Hitachi Remote Ops Monitor Agent, i.e. the amount of bandwidth it has to support monitoring devices, may be viewed in the graphical *Poll Load* function available through the *About* function. The graph will indicate whether the Hitachi Remote Ops Monitor Agent was able to contact every device within the expected scan interval time frame. It will indicate the current load, peak load, and indicate if it was overloaded.

The Hitachi Remote Ops Monitor Agent may be tuned to support more devices by increasing the scan interval. The default interval is 150 seconds (2.5 minutes) but this can be changed up to a maximum of 3600 seconds (60 minutes). If it is set to 60 minutes for example, then it will be able to support many more devices but will have a resolution of 60



minutes on detecting error conditions. It is recommended to choose a value that will not cause the Hitachi Remote Ops Monitor Agent to be overloaded yet will still permit an acceptable error detection resolution. It is recommended to leave the scan interval value at the default setting of 150 seconds unless there's a need to change it for tuning.

The polling interval may be changed for each device - see the section: Starting and Operating the Hitachi Remote Ops Monitor Agent->Device Polling.

Hitachi Remote Ops Monitor Agent Installation Instructions

Use the installation procedures in this section to install the Hitachi Remote Ops Monitor Agent.

- **Windows Installation**

1. The application must be installed via an account with administrative privileges. Run the **MonitorAgentInstaller.exe** application on the Hitachi Remote Ops Monitor Agent distribution.
2. The installation program will start running. Follow the directions in the installation windows to install the Hitachi Remote Ops Monitor Agent. The installation program will install the program in \Program Files\hds\hitdfmon by default. It is recommended to accept the default but it is possible to change the location of the program if desired. The program will be installed and started as a Windows service.

- **Linux Installation**

1. Use the Linux64 directory for 64 bit Linux installations. Run the **HTinst.bin** program (located on the CD in the Linux64 directory) through a terminal window (sh HTinst.bin - note that Unix is case-sensitive).
2. The installation program will start running. Follow the directions in the installation windows to install the Hitachi Remote Ops Monitor Agent. It is recommended to accept the defaults but it is possible to change the location of the program if desired. The installation program will install the program in /usr/hds/hitdfmon by default and will configure the system to automatically start the Hitachi Remote Ops Monitor Agent whenever the host platform starts up (reboot). It does not automatically run the program after the installation completes. The program can be started by launching the **rundfmon** program with the start parameter (sh rundfmon start) located in the installation directory (/usr/hds/hitdfmon by default).

Proceed to the [Starting and Operating the Hitachi Remote Ops Monitor Agent](#) section.

Hitachi Remote Ops Monitor Agent Version Upgrade Instructions

Use the upgrade instructions in this section to upgrade an existing version of the Hitachi Remote Ops Monitor Agent to a new version. Using this procedure, existing settings and device definitions will be retained.

- **Windows Upgrade**

1. Install the updated Hitachi Remote Ops Monitor Agent version by inserting the CD in the drive (it should auto-run) or by invoking the **MonitorAgentInstaller.exe** application.
 - Previous versions of the agent will be uninstalled automatically.

- **Linux Upgrade**

1. Stop the Hitachi Remote Ops Monitor Agent, if running, by running "sh rundfmon stop" in the installation directory (/usr/hds/hitdfmon by default).
2. Uninstall the existing version:
 - If upgrading from version 7.8 or later: Run "sh UninstallHiTrackMonitor" in the /usr/hds/hitdfmon (by



default) directory.

- If upgrading from version 7.7 or earlier: Run "sh Uninstall_Hi-Track_Monitor" in the /usr/hds/hitdfmon/UninstallerData (by default) directory.

3. Install the new version by entering 'sh **HTinst.bin**' through a terminal window.

Starting and Operating the Hitachi Remote Ops Monitor Agent

Initial Running of the Hitachi Remote Ops Monitor Agent

When the Hitachi Remote Ops Monitor Agent is run on the host platform for the first time, various configuration items will need to be set. All configuration is performed through the program's browser interface.

The basic sequence of the steps for configuring the Hitachi Remote Ops Monitor Agent will be -

- Login to the Hitachi Remote Ops Monitor Agent from a web browser.
- Enter the SiteID in the Configuration->Base page.
- Enter the transport information in the Configuration->Transport Agents page to specify the method used to send the data.
- Create any needed device access credentials by using the User Management page.
- Add devices to be monitored via the *Add a Device* or *Item* hyperlink on the Summary page.

The following steps outline the details of configuring the Hitachi Remote Ops Monitor Agent to monitor the devices -

1. Access the Hitachi Remote Ops Monitor Agent from a web browser

Access the application by browsing to the IP address or name of the host platform and specifying port **6696** (the http port the Hitachi Remote Ops Monitor Agent is using by default although it's configurable). For example, if the ip address of the host platform is 123.456.789.001, then browse to: <http://123.456.789.001:6696>. If using a browser on the same host platform as that running the Hitachi Remote Ops Monitor Agent and if the host platform is configured to resolve localhost, it should be possible to access it by browsing to: <http://localhost:6696>. If unsuccessful at connecting to the Hitachi Remote Ops Monitor Agent with the browser, check to make sure the Hitachi Remote Ops Monitor Agent program is running, that the browser proxy settings allow access to the host platform, that network connectivity to the host platform exists, and that HTTP access to the host platform isn't blocked by a firewall. To check if the program is running on Windows, check that the "Hitachi Remote Ops Monitor Agent" service is running in 'Services' under the 'Control Panel'.

2. Log in to the Hitachi Remote Ops Monitor Agent

Log in as an administrator by selecting 'Administrator' from the list box then keying in the password. The default password for both the administrator and monitor access levels is **hds**.

3. Configure the Hitachi Remote Ops Monitor Agent application

The **Configuration selection** allows for entering and changing various configuration items relating to the Hitachi Remote Ops Monitor Agent. The configuration section consists of several pages selectable by clicking the



navigation buttons labeled *Base*, *Transport Agents*, etc. that appear under the *Configuration* heading. The Base page is the first page presented when the configuration page was selected. It's recommended to leave most items at their default values but the following items are required to be set. When completed with the changes on each Configuration page, click the *Submit* button on the page.

- **Base Configuration Page**

- **SiteID:** Enter the 7 character Site ID for this site. It's important that a valid SiteID is set and that it matches the associated setting for the Hitachi Remote Ops site ID in the Hitachi Vantara CRM system so that cases will be created appropriately and notifications performed correctly. If you're not certain of the Hitachi Remote Ops site ID for the site contact the appropriate service/support personnel to determine it. Do not enter an invalid or incorrect site ID.

Note: The SiteID entered in this location will be the default SiteID for devices yet to be configured. It's possible to override this default SiteID for a particular device by setting it on the configuration page for that device. If this default SiteID is changed at a later time, it will NOT affect devices already configured. Those devices already configured would need to have their SiteIDs changed individually if it's desired to change to the new value. This feature allows one Hitachi Remote Ops Monitor Agent instance to monitor devices with different Site IDs if necessary - for example if some devices were in different geographical locations but connectivity to them exists on the customer network.

- **Report Communication Errors:** The default option is to not report errors relating to communication errors between the Hitachi Remote Ops Monitor Agent and the device. This is so that customer network errors don't result in unwanted case opening/notification. If it's desired to report these types of errors, enter a YES here. If it's desired that communication errors result in only an email being sent to the configured email destinations (see next step) but not the Hitachi Remote Ops Center at Hitachi Vantara, enter 'Local'.
- Click on the **Help on this table's entries** link on the page for further detail about the other entries in the table if desired but the other items can generally be left at their default values (recommended).

- **Transport Agents Configuration Page**

- **Always configure all of the transport destinations** for a given transport protocol to provide adequate redundancy - ex: HTTPS to ushtinet01, ushtinet02, usdenhtinet01, usdenhtinet02.
- **HTTPS is the recommended transport** since this will enable advanced functionality such as centralized dump/log requests and provide encryption of the transport. The support for FTP, FTP-SSL is being phased out so configure only HTTPS.
 - Starting in version 8.7, new FTP/FTPS methods can no longer be configured but existing ones can still be modified.
- **The transport connectivity may be tested** independently of Hitachi Remote Ops Monitor Agent by performing the basic connection to the transport destination from the Hitachi Remote Ops Monitor Agent host platform. If using HTTPS as the transport type (recommended), one can browse to the destination - ex: <https://ushtinet01.hds.com> and see if they get a resulting web page versus no connection. If using FTP standard or FTP-SSL one can use a command line application to test the connectivity. Note that the native Windows command line FTP program only supports FTP standard (not SSL) and only supports 'Active' (not Passive).
- **Simplest option - Standard Transport Destinations** - Pre-populated transport methods and destinations have been provided in the selection drop down list next to the 'Create' button. Selecting the transport via the pre-populated transport method is the simplest way to configure the transport. If required by the site's network, configure the proxy information for the transfer method after selecting a transport method/destination and for FTP uncheck the 'Passive' checkbox if required by the customer's network (otherwise leave it checked). This proxy information must be provided by the customer. In many cases a



proxy won't be needed. If the simple destinations are configured then the following details for configuring the methods/destinations manually can be skipped. Be certain to configure all available transport destinations (4 destinations at this point in time).

- **If using the HTTPS (manual) selection** - This option isn't normally needed but is provided for unusual circumstances. The pre-populated destinations described above should be used rather than this option if possible. Enter the HTTPS parameters to allow the monitor program to access the Hitachi Remote Ops Transfer servers at the Hitachi Remote Ops center at Hitachi Vantara. If a proxy will be used, consult with the customer network administrator to determine the proper HTTPS proxy setup. The Hitachi Remote Ops HTTPS Transfer Server will use port 443 for the transport so the customer must make sure their firewall allows the data connection to function through this port (most customer networks already permit this).
 - Under the *Data Transfer Agents* heading, select *HTTPS* in the list box and click the *Create* button. The Configuration page will reappear with a detailed HTTPS configuration form at the bottom.
 - Enter the HTTPS Server to send the data to under *Server*.
 - Select the ethernet interface to use for the HTTPS transport to the public internet under *Local Interface*. If the host platform has multiple interfaces (multiple NIC cards installed), be certain to select the interface that has the access to the public internet. NOTE - If the customer makes later configuration changes to the host platform, it's possible it may affect the interfaces available and that this setting will need to be changed.
 - Enter the HTTPS port to use. This should normally be set to 443.
 - Enter the HTTPS user name under *UserName* (obtain the user names from Hitachi Vantara).
 - Enter the HTTPS Password under *Password* (obtain the passwords from Hitachi Vantara). Note - The password will need to be entered twice, once in each of the boxes adjacent to the *Password* line. Both of these passwords must match.
 - If the customer requires the use of a Tunnel or SOCKS **proxy**, select from the listbox the proxy type and then fill in the appropriate proxy settings in the form. Proxy setting details must be obtained from the customer.
 - Click the *Submit* button to make the changes take effect.
- **If using the FTP (manual) selection** - This option isn't normally needed but is provided for unusual circumstances. The pre-populated destinations described above should be used rather than this option if possible. Enter the FTP parameters to allow the monitor program to access the Hitachi Remote Ops FTP Transfer server at the Hitachi Remote Ops center at Hitachi Vantara. If the customer requires that communications take place through an FTP Proxy, it may be possible to configure the Hitachi Remote Ops Monitor Agent to function through the proxy by manipulating the FTP location and FTP user name. An example FTP proxy setup for the customer Acme might be: FTP Location - ftp.acme.com, FTP User - (normal user)@hitachimon.hds.com, FTP Password - (normal password). If a proxy will be used, consult with the customer network administrator to determine the proper FTP setup. When the FTP connection is set to Passive, the Hitachi Remote Ops FTP Server will use port 21 (non-SSL) or 990 (SSL) for the control connection and will use a port from the range of 50000-50024 for the data connection. The customer must make sure their firewall allows the data connection to function through this port range.
 - Under the *Data Transfer Agents* heading, select *FTP* in the list box and click the *Create* button. The Configuration page will reappear with a detailed FTP configuration form at the bottom.
 - Enter the FTP Server to send the data to under *Server*.
 - Select the ethernet interface to use for FTP'ing to the public internet under *Local Interface*. If the host platform has multiple interfaces (multiple NIC cards installed), be certain to select the interface that has the access to the public internet. NOTE - If the customer makes later configuration changes to the host platform, it's possible it may affect the interfaces available and that this setting will need to be changed.



- Enter the FTP port to use. This should be set to 21 for non-SSL FTP and to 990 for SSL FTP.
 - Enter the FTP user name under *UserName* (obtain the user name from Hitachi Vantara).
 - Enter the FTP Password under *Password* (obtain the password from Hitachi Vantara). Note - The password will need to be entered twice, once in each of the boxes adjacent to the *Password* line. Both of these passwords must match.
 - If the customer requires the use of a Tunnel or SOCKS **proxy**, select from the listbox the proxy type and then fill in the appropriate proxy settings in the form. Proxy setting details must be obtained from the customer.
 - If SSL transport is to be used, select from the listbox the SSL alias name "Hitachi Vantara FTP".
 - Click the *Submit* button to make the changes take effect.
- **Device Polling**
 - Leave this setting at the default unless there's a specific reason to change it to decrease the frequency of polling for errors. This would generally only be needed if there is a performance issue with Hitachi Remote Ops Monitor Agent communicating with all of the devices due to a large number of devices defined, a slow customer network, or related issues.
 - This table shows an entry for each type of device and allows the user to define a multiple of the polling interval for that device type. For example, if the polling interval is 150 seconds and a multiple of 3 is defined for a device type then that device type will be polled every 450 seconds.
 - The table also shows the equivalent import/export name for the device type as a reference for the device type name in the 8th column of the import/export file.
 - The 'Disable' column allows the device type to be removed from the list shown in the Add Device page.
 - Click on the 'Help on this table's entries link (above the table) for more details.
 - **Local TCP/IP Configuration Page**
 - Leave this setting at the default unless there's a specific reason to change it.
 - The **HTTP/SNMP Service Ports** may be changed if needed but generally the default values will be used.
 - The **Sftp Server (Daemon)** section is used to provide support for the Brocade Support-Save function. This function must use local TCP port 22. If the host is already using TCP port 22 then it's not possible for Hitachi Remote Ops Monitor Agent to perform the Support-Save function and the local interface for this service must be set to '*NOT_SET*'. If local TCP port 22 is available then the Sftp service may be configured. Only one local interface may be configured and its local interface must be accessible by the Brocade switch. Hitachi Remote Ops Monitor Agent only checks this interface during startup so if a change is made here restart the Hitachi Remote Ops Monitor Agent to enable the service on a specific interface.
 - The **Local TCP/IP Interface** may be changed if need be to match the interface (network) that the devices to be monitored are on. This generally only needs to be changed if the host platform has multiple NICs installed and the default selection is the wrong interface to be able to communicate with the devices. If after completing the configuration of the Hitachi Remote Ops Monitor Agent it's unable to communicate with the devices, then this setting is likely pointing to the wrong interface and needs to be changed to the correct one.
 - Click the *Submit* button to make the changes take effect.
 - **Debug/Trace Configuration Page**
 - Leave this setting at the default unless there's a specific reason to change it.
 - This page is used to increase the level of logging for troubleshooting problems. This page should generally be left at its default values unless a problem is encountered that requires an increased logging level.



- **Timezone Configuration Page**

- Leave this setting at the default unless there's a specific reason to change it.
- This page is used to change the timezone settings. This page should generally be left at its default values unless a problem is encountered with the timezone setting.

- **Email Configuration Page:** The Hitachi Remote Ops Monitor Agent can optionally send email notifications to a user defined list of email locations. The customer must supply the name or IP address of the sending mail server to use. Email locations to send the notifications to are entered in the User List and are separated by a comma. Some customer mail servers won't allow an email to be sent unless the sender's email address is already known to it. In this case, set the *Sender's Email Address* area up with an email address that's known to the sending mail server. This address must be supplied by the customer. Use SSL Mode=Automatic and Authentication Mode=User/Password for third party email sites such as Google(tm) mail. Specify an SMTP User and Password if required by the mail server at this site. Click the adjacent *Submit* button to make the changes take effect. Click the *Test Email* button to have a test email sent to the locations just configured. Note that this email function is optional and used only for the customer's convenience. It doesn't affect the normal communication path to Hitachi Vantara for the purpose of notifying Hitachi Vantara service personnel.

- **Backup Tab**

- The Hitachi Remote Ops Monitor Agent can function in a primary/backup mode for redundancy if desired. In this mode the backup instance communicates with the primary instance and if the primary instance is non-responsive the backup instance will start polling the devices for error conditions and report them until the primary becomes responsive again. This is an optional configuration item. It's not required to have a backup instance.
- The 'Backup Tab' allows a *Primary* Hitachi Remote Ops Monitor Agent to be defined if this instance will be a *Backup* instance. Don't configure anything on this page if this instance is the primary.

- **User Management Page**

This function allows for **entering and changing passwords** used for logging onto the Hitachi Remote Ops Monitor Agent, for setting account authentication credentials for HUS, AMS2000, and certain other storage devices that support the function, for setting credentials to access SNMP devices, for setting up a Proxy and SSL, and for setting other device specific connection credentials. This function is used to configure the user/password information required to access SNMP v3 devices such as Cisco and HCP-AW/HCP, and to set access credentials for FTP and Telnet for other devices such as the Compute Blade Server 2000 and 320, and to set Remote User credentials for HNAS. It's also used to configure SNMP community strings to access devices such as Brocade and HCP-AW/HCP. The typical default SNMP community string of "public" is already configured so if that's the only one configured into the devices, no additional configuration is required on this page for those devices. The SSL security information should normally be left at its default value and not require any setting.

The settings for the various credentials typically require making up a 'Security Name' alias as a reference to the object. This alias name that will be used to associate the security credentials can be anything such as "mySOCKS", "Hitachi", "HiTrack", HTTPS_Proxy, CiscoDevices, etc. The UserID and Password entered here must match those configured on the device for the access Hitachi Remote Ops requires. Note that certain default credentials are already defined for certain device types.

- **Changing the Hitachi Remote Ops Monitor Agent login password**

- One may configure the Hitachi Remote Ops Monitor Agent user interface access to be via local credentials or Active Directory credentials. If Active Directory is to be used then the appropriate Domain, Server Name, and Organizational Unit, and SSL Mode need to be configured in the form and it needs to be enabled. If not using Active Directory this form should indicate 'Enabled - False' and the other form for the local credentials used.
- Select *Monitor User* from the security object listbox and click the adjacent *Refresh* button.



- Select the Monitor User Type in the *Define Monitor User Types* table by selecting the appropriate radio button and then clicking the adjacent *Refresh* button.
- If using local authentication enter the desired password to use in the *Detail for Monitor User* table and click the adjacent *Refresh* button. If using Active Directory authentication fill out the fields in the second form.
- **Setting the GUM (controller) and SVP user IDs for VSP F/G 900/700/370/350/130 or VSP E990**
 - This device type requires the configuration of a user/password to access the GUMs (controllers) and one to access the SVP (if present). A default value exists for the GUMs but if the default was changed in the device then a new object with matching credentials must be created here. The default for the GUMs is object name 'VSP G/F130, G/F350, G/F370, G/F700, G/F900 GUM'. The SVP doesn't have a default so a new *Remote User Id* object must be created for it.
 - Select *Remote User Id* from the security object listbox and click the adjacent *Refresh* button.
 - Enter an alias name in the box under *Security Name*. This name is an alias that will be used to reference the security information to be added in the next step. After entering the name, click the adjacent *Refresh* button.
 - In the *Detail for Remote User Id* table at the bottom of the page, enter the Remote UserID to be associated with the name just entered in the previous step. The Remote UserID defaults to be the same as the Security Name but the Remote UserID may be changed here if needed. In the Remote Password field enter the password for the associated user ID. After entering the information, click the adjacent *Refresh* button.
- **Setting the account authentication credentials for HUS, AMS2000**
 - The HUS and AMS2000 devices use *account authentication* by default and some other Hitachi storage device types may also have been configured to use it although it's not the default for these other devices. Account authentication is configured in the device via Storage Navigator Modular 2. Consult the Storage Navigator Modular 2 and device documentation for details on the account authentication function. For devices configured to use account authentication the Hitachi Remote Ops Monitor Agent must be configured to match the credentials configured in the device. Normally one would configure the device with a *hitrack* account that has *view only* privileges meaning it can only read certain configuration information but can't change the configuration. The HUS and AMS2000 devices should have a default *hitrack* account already configured. Some customers might choose to change the credentials from the default. Since it's possible that the default isn't configured for the device, it must be checked to ensure it's set. The Hitachi Remote Ops Monitor Agent already has the default account authentication account ID configured for HUS and AMS2000 devices. If the default setting will be used, then the step to configure the account ID in *User Management* can be skipped.
 - **To use the default account authentication setting in Hitachi Remote Ops Monitor Agent** -When defining a new device to be monitored select the *AMS2000 Default* selection in the *Account ID* field for the device. Use this setting for both HUS and AMS2000 types of devices.
 - **To configure the account authentication into the device** - using Storage Navigator Modular 2, select the *Security -- Account Authentication* function and see if there's an account with the name *hitrack* for the particular device. If there is, then the default ID is likely already configured for the device (if the password is also configured to the default one) and the steps to configure an account into the device via Storage Navigator Modular 2 can be skipped.
 - If the default ID wasn't already set for the device it must be set now. Using Storage Navigator Modular 2, access the *Security -- Account Authentication* function, click the *Add Account* button to add an account, and create an account with the following:
 - User: **hitrack**
 - Password: **hitachi**



- Account: **Enable**
- Role: **Storage Administrator (View Only)**
- **To configure a non-default account authentication account into the *Hitachi Remote Ops Monitor Agent*** - in the Hitachi Remote Ops Monitor Agent, select *User Management*, select *AMS/WMS/SMS Account Id* under the *Select type of Security Object to display* function and then click the adjacent *Refresh* button.
- The currently defined account ID security objects are displayed. Add a new one by entering the new account name in the *-Add New User Here-* box under the *Security Name* column and then click the adjacent *Refresh* button.
- After *Refresh* was clicked in the previous step, there will be a new section at the bottom of the page indicating the detail for the particular user name. In this table enter the *Account Name* and *Password* associated with the *Security Name* and check the *Default* box if this will be the default setting for this site and will, for example, be used for all the devices at this site with account authentication enabled.
- **Setting the SNMP v3 user/password information (use for Cisco and optionally for HCP-AW/HCP or other devices configured to use SNMP v3)**
 - Select *SNMP v3* from the security object listbox and click the adjacent *Refresh* button.
 - Enter an alias name in the box under *Security Name*. After entering the name, click the adjacent "Refresh" button.
 - In the *Detail for SNMP v3* table at the bottom of the page, enter the Authorisation User and Authorisation Password to be associated with the name just entered in the previous step. The Authorisation User defaults to be the same as the Security Name but the Authorisation User may be changed here if needed. For example, if the Cisco devices have their SNMP v3 parameters configured with "administrator" as the authorisation user and "administrator123" as the authorisation password, then the following might be set in this table: Security Name: MyCisco, Authorisation User: administrator, Authorisation Password: administrator123. After entering the information, click the adjacent "Refresh" button.
 - The Authorisation Protocol default of HMAC-MD5-96 should not be changed without checking the device configuration.
- **Setting the SNMP community string information (use for Brocade and optionally HCP-AW/HCP).**
 - Select *SNMP* from the security object listbox and click the adjacent *Refresh* button.
 - Enter an alias name in the box under *Security Name*. After entering the name, click the adjacent *Refresh* button.
 - In the *Detail for SNMP Community* table at the bottom of the page, enter the Community ID to be associated with the name just entered in the previous step. The community ID defaults to be the same as the Security Name but the community ID may be changed here if needed. After entering the information, click the adjacent *Refresh* button.
- **Setting the HCP 'HCP Log' Remote User ID**
 - Select Remote User ID from the security object listbox and click the adjacent Refresh button.
 - Create a new Remote User ID can be created by replacing *-AddNewUser Here-* with an alias name for this security object, and click Refresh.
 - The HCP Log is fetched from the HCP via the HCP API so the Hitachi Remote Ops Monitor Agent needs to have a 'Remote User ID' be configured with the user ID and password that are configured on the HCP for the API. Each password must be entered twice. Click Refresh to add this new security object.
 - This security object can then be selected in an HCP add/modify page to associate this security object



with the particular device.

- **Setting the Compute Blade Server Dump Fetch Id**

- Select Dump Fetch Id from the security object listbox and click the adjacent Refresh button.
- A default dump id exists which cannot be edited. A new Dump Id can be created by replacing -AddNewUser Here- with an alias name for this security object, and click Refresh.
- The dump is fetched from the Compute Blade Server via telnet and FTP so the Hitachi Remote Ops Monitor Agent needs to have a 'Dump Fetch ID' be configured with the telnet and FTP information configured on the Compute Blade server. If telnet and FTP aren't already configured on the Compute Blade server then they need to be configured on the device. Enter the Telnet UserID and Telnet Password that will be used to request a new dump from the Compute Blade, and the FTP UserID and FTP Password that will be used to fetch the dump from the Compute Blade. Each password must be entered twice. Click Refresh to add this new security object.
- This security object can then be selected in a Compute Blade add/modify page.

- **Setting the Logon Username/Password for HNAS SMU.**

- A default ID *SMU* is predefined for a standard SMU configuration with a userID of *manager* and the default password. If this SMU is using the default access credentials then a new Remote userID security object isn't needed but otherwise, follow the next steps to create a new security object for the device. If the customer changed this credential on the SMU then the customer will need to provide or enter the new userID/password.
- Select *Remote User Id* from the security object listbox and click the adjacent *Refresh* button.
- Enter an alias name in the box under *Security Name*. This name is an alias that will be used to reference the security information to be added in the next step. After entering the name, click the adjacent *Refresh* button.
- In the *Detail for Remote User Id* table at the bottom of the page, enter the Remote UserID to be associated with the name just entered in the previous step. The Remote UserID defaults to be the same as the Security Name but the Remote UserID may be changed here if needed. In the Remote Password field enter the password for the associated user ID. After entering the information, click the adjacent *Refresh* button.

- **Setting the Logon Username/Password for HPP.**

- A default ID *HPP* is predefined for a standard HPP configuration with a userID of *hitrack* and the default password. If this HPP is using the default access credentials then a new Remote userID security object isn't needed but otherwise, follow the next steps to create a new security object for the device. If the customer changed this credential on the SMU then the customer will need to provide or enter the new userID/password.
- Select *Remote User Id* from the security object listbox and click the adjacent *Refresh* button.
- Enter an alias name in the box under *Security Name*. This name is an alias that will be used to reference the security information to be added in the next step. After entering the name, click the adjacent *Refresh* button.
- In the *Detail for Remote User Id* table at the bottom of the page, enter the Remote UserID to be associated with the name just entered in the previous step. The Remote UserID defaults to be the same as the Security Name but the Remote UserID may be changed here if needed. In the Remote Password field enter the password for the associated user ID. After entering the information, click the adjacent *Refresh* button.

- **Setting the Logon Username/Password for UCP Director, UCP Advisor, HCP S Series Node (HCP-S), HCP-CS, Hitachi Content Intelligence (HCI), Hitachi Advanced Server 8x0.**

- There is no default ID defined for these device types. The user must define a new Remote User Id



object as shown above for new HNAS userID/passwords.

- **Setting the Proxy information (only used if the customer requires going through a Tunnel or SOCKS proxy server for internet access)**
 - **NOTE:** The proxy setting procedure is now performed in the transport setup form on the Transport Agents page rather than in the User Management page. The steps below are for down level compatibility but if configuring a new proxy, do it from the Transport Agents page.
 - Select *Proxy* from the security object listbox and click the adjacent *Refresh* button.
 - Enter an alias name in the box under *Security Name*. This name is an alias that will be used to reference the security information to be added in the next step. After entering the name, click the adjacent *Refresh* button.
 - In the *Detail for Proxy* table at the bottom of the page, enter the security information associated with the Proxy server. This information must be provided by the customer. After entering the information, click the adjacent *Refresh* button.
- **Setting the SSL information (only used if the SSL FTP transport is to be used).** NOTE: At this time, leave the SSL setting at its default values. No changes are necessary for SSL to function.
- **Setting the Remote User Username/Password for Brocade and Cisco Diagnostic / Dump Fetch:** A 'Remote User Id' must be created before the Brocade Support-Save or Cisco Tech-Support requests can be performed. The same Remote User Id may be used for Brocade and Cisco devices. There is no default Remote User Id. Select *Remote User Id* from the security object listbox and click the adjacent Refresh button. Enter an alias name in the box under 'Security Name'. After entering the name, click the adjacent *Refresh* button. In the 'Detail for Remote User Id' table at the bottom of the page, enter the Remote UserID to be associated with the name just entered in the previous step. The Remote UserID defaults to be the same as the Security Name but the Remote UserID may be changed here if needed. In the *Remote Password* field enter the password for the associated user ID. After entering the information, click the adjacent *Refresh* button.
- **Setting the Remote User Username/Password for the Hitachi Advanced Server DS7000:** A 'Remote User Id' must be created to access the BMCs of the DS7000 server. There is no default Remote User Id. Select *Remote User Id* from the security object listbox and click the adjacent Refresh button. Enter an alias name in the box under 'Security Name'. After entering the name, click the adjacent *Refresh* button. In the 'Detail for Remote User Id' table at the bottom of the page, enter the Remote UserID to be associated with the name just entered in the previous step. The Remote UserID defaults to be the same as the Security Name but the Remote UserID may be changed here if needed. In the *Remote Password* field enter the password for the associated user ID. After entering the information, click the adjacent *Refresh* button.
This Username/Password must match what's set on the DS7000 server for access to the BMC ports. The settings on the DS7000 must permit 'IPMI' access as an 'Operator' (for added security).

4. Add devices to be monitored

Devices to be monitored may be added, deleted, edited and their status viewed on the **Summary page**. Devices (HUS, AMS, HNAS, HCP, Brocade switch, etc.) to monitor are added by clicking on the *Add a Device* or *Item* hyperlink on the device summary page (this operation requires that the user be logged on to Hitachi Remote Ops Monitor Agent as Administrator). After the *Add Device* page is presented, select a device type from the list box and then enter the details for the particular device to monitor. After entering the details, click the *Add* button to make the changes effective. Repeat this process by modifying the form for a similar device and clicking *Add* or by selecting a different type of device from the list box. When done entering units, select the *Summary* navigation button to return to the device summary screen. The entry form will vary somewhat by device type since different device types may have different requirements. The following pertains to a typical device



type.

- **Name, Location, Group:** These are optional fields and are used only as a reference for conveniently identifying the particular unit on the device summary page and in the data sent to the Hitachi Remote Ops center. They may be left blank if desired but it's recommended to use one or more of these fields to identify the particular device in a meaningful way.
- **Serial:** If this field doesn't exist on the form then for this type of device the serial number will automatically be sensed from the device. If the form has a serial number field in it then the serial number must be manually entered. For some devices, such as Brocade, a "Use Soft-Serial" checkbox will appear. Checking this box will force the agent to attempt to read the serial number from the device rather than the user needing to enter the serial number in the 'Serial' field.
- **Site ID:** The default SiteID that was previously entered in the Basic Configuration page will appear here. If it's desired to have a different SiteID for this unit in order to have different siteIDs for different devices in a single instance of Hitachi Remote Ops Monitor Agent, generally when the monitored devices are in different geographical locations, overtype this SiteID with the appropriate and correct one. Make certain that a valid SiteID exists in this field. If you don't know the correct site ID for the site or device contact Hitachi Vantara to obtain it. This siteID needs to be correct for the device.
- **IP Address 1 (and IP Address 2):** This is a required field. Enter the IP address (or resolvable name) of the device to be monitored. For storage devices this is the IP address of the controller(s). For switches, this is the IP address of the unit responding to SNMP requests. For HCP-AW/HCP, this is the IP address of the nodes. For HNAS, this address needs to be set to the IP address of the SMU. If more than a single IP address field exists on the form enter the IP addresses of the multiple paths to the device so communications can continue to occur if, for example, one of the controllers is non-responsive.
- **Local Interface:** For host platforms with multiple network interfaces, select the appropriate network interface to use to communicate with the device. If it's unknown which interface to select leave it as is and only change it if the Hitachi Remote Ops Monitor Agent is unable to communicate with the devices.
- **Comms Error Reporting:** This field allows for overriding the default value for this device regarding reporting communication errors that was set previously in the Configuration setup.
- **Enabled?:** This checkbox determines whether the device will be enabled for monitoring. This should normally be left checked.
- **Trace:** This checkbox determines whether trace the device at an enhanced level for troubleshooting purposes. Normally this should be left unchecked unless directed to check it by a service person.
- **SNMP Access ID:** This field is only for devices where the interface to Hitachi Remote Ops Monitor Agent is via SNMP (refer to table under *Prerequisites*). Enter the SNMP alias name from the droplist. These alias names are defined through the *User Management* function previously described.

Refer to the following device specific configuration items and notes depending on the particular device type being configured.

- **VSP F/G 900/700/370/350/130, VSP E990**
These devices are monitored via multiple interfaces. Enter the IP addresses/names of both GUMs (controllers) and the SVP (if present). The associated Remote Access ID alias (configured earlier in the 'User Management' function) must be selected for GUM and SVP.
- **HCP-S, HCP, HCP-AW system**
These systems are treated in Hitachi Remote Ops Monitor Agent as different types of devices due to the way they respond to the application.
The HCP-AW/HCP system may have multiple nodes as potential access points. It's recommended to configure two nodes into a single 'Add a Device' entry box so that if one node fails the agent will still be able to communicate through the other node. The status of all nodes is reported through each node so it's not necessary to have Hitachi Remote Ops Monitor Agent through each node. An example would be that a 4 node



system would have just two nodes configured as the IP addresses in a single *Add a Device* box for the HCP-AW/HCP system.

The HCP is monitored via SNMP protocol and HTTP protocol to the HCP API. The API is used to acquire the 'HCP Log'. Hitachi Remote Ops Monitor Agent needs to be configured with the appropriate user ID and password that matches the user ID and password required by the API of the HCP. The user ID and password in Hitachi Remote Ops Monitor Agent are configured by adding a 'Remote User ID' in the User Management tab of Hitachi Remote Ops Monitor Agent. See the description of this User Management function in a preceding section.

- **HNAS system**

The current method Hitachi Remote Ops Monitor Agent uses to monitor the HNAS system is via the SMU method. Previously supported methods of monitoring the HNAS via SNMP and by the device sending an email directly to Hitachi Remote Ops at Hitachi Vantara are no longer supported.

- **To configure the SMU method** - select *Hitachi NAS (HNAS) Server Management Unit (SMU)* from the *Select Device Type* list. Define the IP address for the SMU and select the appropriate Remote User alias (configured in *User Management previously*). When Hitachi Remote Ops Monitor Agent communicates successfully with the SMU it will discover and automatically add the HNAS clusters (servers) accessible via this SMU. Those clusters will then also appear in the list of monitored devices as well as the SMU.
- **Note** - It's possible there could be multiple SMUs configured with the same clusters when the SMUs are in an active/standby redundant type of configuration. Hitachi Remote Ops Monitor Agent should be configured to point to only the 'active' SMU so the agent will end up with only a single instance of any cluster.
- **Note** - The *Hitachi NAS (HNAS) Server* device type exists to Modify the clusters that were automatically discovered and added after communicating with the SMU as outlined above. This selection allows for modifying the device including the Name, Location and Group fields. Don't select this option from the list for the purpose of adding a device.
- **Note** - The *Hitachi NAS (HNAS) Platform* from the *Select Device Type* list was used only for the now obsoleted SNMP based monitoring method so don't use this selection.

The HNAS device may be configured to require particular communications **ciphers** and if a non-default cipher is configured for the HNAS then the similar cipher must be defined in Hitachi Remote Ops Monitor Agent on the 'Configuration' tab in the text box 'HNAS Ciphers'. This field may be left blank unless the HNAS was configured for a non-default cipher. The 'help' link for the page defines the ciphers that may be used.

- **Quanta server**

The Quanta server nodes each have a BMC port and a customer network port. When adding a Quanta device to be monitored, configure Hitachi Remote Ops Monitor Agent with the 'BMC port' addresses of each server node in the Quanta system.

- **Hitachi Advanced Server DS7000**

The DS7000 server nodes (modules) each have a BMC port and a customer network port. When adding a DS7000 device to be monitored, configure Hitachi Remote Ops Monitor Agent with the 'BMC port' addresses of each node (module) in the DS7000 system.

- **CB 2500 and CB 500 Servers**

These systems have a limitation that only two client IP addresses can access it total even if one of them is no longer accessing it. If there are no available sessions Hitachi Remote Ops Monitor Agent will indicate "Too many concurrent sessions" in the status for the device. In order to permit the agent to access it in this case one must log into the CB2500/CB500 Web Console and view the Administration->Hi-Track->Hi-Track Servers, view the IP addresses, and delete one of them by selecting one of them and clicking 'Delete' in the bottom right of the page. The Hitachi Remote Ops Monitor Agent will automatically be registered once it



communicates with the CB2500/CB500 and there's room for its IP address. Optionally, the IP address may be added via the CB2500/CB500 Web Console.

- **CB2000**

When the security strength level on the CB 2000 Management Module is set to 'High,' the agent will only use SNMPv3. If you do not or cannot use SNMPv3, and can only use SNMPv1/v2c, make sure the security strength level on the CB 2000 is set to 'Default.' To check and/or change the current security strength level, use the SC command at the CB 2000 CLI console. For detailed information about the SC command, refer to the Compute Blade 2000 USER'S GUIDE, Section 6 titled "Management Module Settings."

- **Hitachi Ops Center Automator (HAD)**

Use the default 'Remote User ID' named 'Hitachi Automation Director' unless the default was changed on the Hitachi Ops Center Automator product. If a different user ID will be used use the following procedure:
A User ID must be defined from the 'User Management' Tab. Select Security Object type 'Remote User Id' and click Refresh. Overtyping *-Add New User Here-* with a new unique identifier for this Security Object (example: HAD1) and click Refresh. In the *Detail for Remote User Id 'HAD1'* add the userId and password that has already been defined on the HAD device and click Refresh. A HAD device may now be defined. Use the Security Name Id in the Remote User field.

- **Hitachi Content Platform for Cloud Scale (HCP-CS)**

A realm name that corresponds to the user account should be configured.

After adding items, wait a few minutes until the program has had a chance to communicate with the device to obtain the data before clicking on the device detail icon. It's possible the program will move the device to 'Not Monitored' if there's a problem reading the serial number or other data from the device. In this case, correct the issue with the serial number, for example, ideally by setting it at the device or optionally, setting it in the Hitachi Remote Ops Monitor Agent device configuration for that device.

Note:

It's possible to import the devices to be monitored from a comma delimited file. This is useful if the Hitachi Remote Ops Monitor Agent will be connected to a large number of devices. The format of the comma delimited file has 13 columns separated by commas with a carriage return/Line feed at the end of the line. The columns consist of:

1. Device Name (free format text)
2. Device Location (free format text)
3. Device Serial Number (free format text - will be overridden for DF, and McData devices)
4. SiteID (7 character Hitachi Remote Ops ID)
5. IP Address 1 (either dotted-decimal or name)
6. IP Address 2
7. Communications Report Value:
 - (blank) (use the globally defined value)
 - CERlocal (Report errors via email only)
 - CERno (do not report communication errors for this device)
 - CERyes (always report communication errors for this device)
8. Device Type (prefacing with NM denotes "Not Monitored"). Note that the 'Device Type' name can also be viewed in the Configuration->Device Polling table.
9. Device Local Interface #1 (e.g. 'eth0')
10. Device Local Interface #2



11. IP Address 3
12. Dump Fetch alias name for Hitachi Compute Blade, HCP-CS, and some other types as defined on User Management page.
13. Security ID (The alias name defined for security attributes on User Management page - (SNMP) Access ID, or the (storage) Account Id), or the Remote User ID (HNAS SMU), or the Security IDs for other monitored products. The HNAS Server via SMU device will put its Index number (used to select it via the SMU) in this field. For HCP-CS this is the realm name.
14. Group name (free form text)
15. IP Address 4

Device	Value
VSP F/G 900/700/370/350/130	hm850
VSP E990	hm900
HUS	hus
AMS2000	ams2k
HCP	hcp
HCP-AW	hcpaw
HCP-S	hcpsx0
HCP-CS	hcpcs
HCI	hci
HDI	hdi
HPP	hpp
HNAS SMU (CLI)	smu



HNAS Server via SMU	hnas-server
UCP Advisor	ucpadv
UCP Director	ucpdir
Compute Rack Server CR xM (CR 2x0H/S)	cr2x0hs
Compute Blade Server CB 2500	cb2500
Compute Blade Server CB 500	cb500
Compute Blade Server 2000, 320, IOEU	symphony
Cisco	cisco
Brocade (except FCX 648)	brocade
Brocade FCX 648	foundry
Quanta	quanta2U
Hitachi Advanced Server DS7000	bull
Hitachi Ops Center Automator	had
Hitachi Advanced Server 8x0	hpe
Generic Fibre Channel	fc

To import the data, stop the Hitachi Remote Ops Monitor Agent program and then run the import program from the installation directory as follows:

- Windows: jre\bin\java -jar HiTrack.jar import commFileName



- Linux: `sh rundfmon import commFileName`

Where `commFileName` is the comma delimited file to import. After importing the file, restart the Hitachi Remote Ops Monitor Agent program. If switch/NAS type devices were defined with non-default alias names (other than 'public' for SNMP or any SNMPv3 device) then for a new Hitachi Remote Ops Monitor Agent install where the alias hasn't already been configured, the alias name will need to be configured in 'User Management' and the devices, which will appear in the 'Not Monitored' section, will need to have their 'Enabled' checkbox checked to allow them to be monitored.

It's possible to export the configuration from the Hitachi Remote Ops Monitor Agent to a comma delimited file by changing the *import* keyword to *export*. An export file (`devices.export`) is produced automatically about every 5 minutes.

Optional Setup Parameters

The Hitachi Remote Ops Monitor Agent program should be running 24/7 to ensure that it will detect error conditions on the monitored devices and so that it can report to the Hitachi Remote Ops center at Hitachi Vantara on a daily basis. Normally the program runs in the background (as a Windows Service or Linux process) and no window is presented for the program. All interaction with the program is performed via web browser access to the monitor program. Through the browser interface one may set basic configuration items, add new devices, or modify or delete existing devices to monitor, view the status of each device, or view details of a device. A web browser anywhere on the customer's network that has TCP/IP connectivity to the host platform running the Hitachi Remote Ops Monitor Agent can typically be used to interact with the program. It's possible to have multiple browsers from multiple locations access the Hitachi Remote Ops Monitor Agent concurrently. The browser access has two operational levels based on the type of login used - Administrator and Monitor. The Administrator type is allowed to set or change basic configuration items and add/edit/delete devices to monitor. The Monitor type is not allowed to set or change program configuration items but can monitor device status and view device details. When a browser is displaying the device summary page, the page will update itself about every 60 seconds.

The top table on the device summary page displays a summary of the numbers of devices that are presently in a particular monitor category which includes devices exhibiting errors, devices that the monitor program is unable to communicate with, devices that are reporting okay and with no errors, devices not monitored due to user setting, and total devices configured for the monitor. The table contains checkboxes which determine what categories will be displayed in the tables that follow this summary table. The default is that all tables will be displayed (checkboxes checked).

Up to four tables will follow the summary table. The following tables are presented if any devices exist in the category:

- **Device Error** - This table displays devices which are exhibiting errors. The Status column will be red with a short summary of the error type.
- **Communication Error** - This table displays devices which the monitor program is unable to communicate with. The Status column will be in yellow. The communication error may be due to a network problem, ip address setup problem, or the device is powered off.
- **Device Okay** - This table displays devices that are reporting normally and exhibit no errors. The Status column will be green.
- **Not Monitored** - This table displays devices that the user specified to not monitor even though they're configured in the monitor. This is performed via a checkbox on the item setup. The Status column will be pale yellow. This option



may be used to disable checking of the device when maintenance is being performed to the device or when a customer has the device temporarily unavailable.

In each of these four tables the following columns are presented:

- **Item** - Indicates the item number for the device according to the order in which the devices were entered. In administrator mode, the item number is hyperlinked and may be clicked to modify the device's monitor setup parameters and the Item heading is hyperlinked to allow for adding new devices when clicked. Note - It may take a few minutes for the data for a newly added device to be obtained before having valid detail data for the device.
- **Name, Location, Group** - Indicates the name, location, or group set when the device was added. This is for user reference only.
- **Type** - Indicates the type of device (DF Storage, Cisco, etc.).
- **Model** - Indicates the model number of the device (HUS, AMS, etc.).
- **Serial** - Indicates the serial number of the device.
- **Status** - Indicates the error status of the device.
- **Last Communication** - Timestamp of the last time the monitor attempted to communicate with the device. This field is normally updated every few minutes.
- **Site ID** - Indicates the Site ID set for the device at the time it was added.
- **IP Address 1 or 2** - Indicates the IP addresses that were set for the device when it was added.

In the *Status* column for a particular device, the 'D' icon may be clicked to display a page showing details of the device. The detail page includes a number of tables showing error status and configuration details for various functional components including drives, cache, power, fans, microcode levels, etc.

The Hitachi Remote Ops Monitor Agent will send device data related to error and device configuration to the Hitachi Remote Ops center when an error condition is detected and also on a daily basis.

Clicking the *Transport History* navigation button will present a page indicating the data transport activity of the Hitachi Remote Ops Monitor Agent. This can be useful for troubleshooting transport problems. This page also has a *Request Report* button at the bottom which will force a data transport to take place. This can be used to ensure the Hitachi Remote Ops Monitor Agent is configured properly to transport the data to the Hitachi Remote Ops Center.

Note: For some program configuration changes, the program will indicate to restart the agent. This is done by stopping then starting the "Hitachi Remote Ops Monitor Agent" service through the Windows Control Panel for Windows systems, or by running "sh rundfmon stop" followed by "sh rundfmon start" for Linux systems.

Before stopping the Hitachi Remote Ops Monitor Agent all polling operations should be stopped by using the **Shutdown** command in the browser interface. This is accessed from the *About* tab, the *SHUTDOWN* option in the left hand menu, and finally by clicking the *Confirm Shutdown* button. This command stops all polling and reporting operations - the Thread Activity display is shown while the current polling operations complete. The threads that are ending are shown with a yellow background. When the display shows that Shutdown is complete then the Hitachi Remote Ops Monitor Agent service may be stopped. The Hitachi Remote Ops Monitor Agent does not terminate when the Shutdown command completes - the browser interface continues to run until the service is terminated.



Optional Setup Parameters

The Hitachi Remote Ops Monitor Agent application can function in various modes other than the basic single instance monitoring mode as well as perform some additional functions not typically configured in most applications.

- **Backup Mode**

The Hitachi Remote Ops Monitor Agent can be configured such that there are two instances of the Hitachi Remote Ops Monitor Agent running on two different host platforms with one acting as a primary and the other as a backup. The devices to be monitored must be defined for both instances. When in backup mode the backup instance doesn't actively monitor the devices but rather, communicates with the primary instance to determine if it's operational. If the primary instance becomes inoperable the backup instance will take over the function of polling and monitoring the devices. The backup will continue to monitor the primary and once the primary becomes operational again the backup will stop monitoring the devices and resume its backup role.

To configure an instance to be a backup instance, go to the *Configuration-Backup* page and enter the URL of the primary instance and click Submit. This is the exact URL as one enters when browsing to the primary - ex:

<http://10.3.4.5:6696/>.

- **File Relay Mode**

Hitachi Remote Ops Monitor Agent can function as a 'File Relay' application (this function is added in version 7.8). In this mode the agent is configured to monitor a particular local directory on the host platform for incoming files and forward those files on to the Hitachi Remote Ops center at Hitachi Vantara and then delete the files. The purpose of this is to assist with network segregation for those sites that require this type of functionality. Most sites do 'not' require this functionality and this function should be avoided if possible since the advanced functionality of centralized dump acquisition and Remote Microcode Update will not function in this configuration. In this File Relay mode the Hitachi Remote Ops Monitor Agent instance would normally be configured to 'only relay files' and not actually monitor devices. The normal scenario would be that one instance of Hitachi Remote Ops Monitor Agent and/or the Hitachi Remote Ops SVP Agent would be configured to monitor devices and then the monitoring agent would transport to the host platform running a second instance of Hitachi Remote Ops Monitor Agent operating in file relay mode. In this configuration the first instance that's monitoring the devices typically wouldn't have internet connectivity to transport the data to Hitachi Vantara directly (or else this File Relay function wouldn't be needed) but the second instance operating in file relay mode would have internet connectivity generally through a different network interface, i.e. the host platform would have multiple network interfaces where one has connectivity to the Hitachi Remote Ops site agents and the other to the internet. This configuration provides a means to accommodate that network configuration.

In this mode the host platform for the Hitachi Remote Ops Monitor Agent operating in this mode must be configured to accept files from the Hitachi Remote Ops Monitor Agent instance that's monitoring the devices. This is typically done via an FTP server running on the host platform of the instance in the File Relay mode and would be provided by the customer. Alternatively the host platform could be configured to receive files via HTTPS. Perform the following steps -

- Configure the FTP (or HTTPS) server on the host platform of the File Relay instance of Hitachi Remote Ops Monitor Agent with a user and password with a particular home directory on that platform.
- Configure the File Relay instance of Hitachi Remote Ops Monitor Agent to that home directory defined in the



step above. This is done on the Configuration ->Transport Agents ->File Relay Configuration section.

- Configure the File Relay instance of Hitachi Remote Ops Monitor Agent to transport to the transfer servers at Hitachi Vantara as described previously in this document.
- Configure the Monitoring instance Hitachi Remote Ops Monitor Agent and/or the Hitachi Remote Ops SVP Agents to transport the files via FTP (or HTTPS) to the host platform of the File Relay instance using the user and password configured for the FTP (or HTTPS) server previously.

• **SNMP Agent**

Hitachi Remote Ops Monitor Agent may be configured to send an SNMP notification upon certain events and may also be queried with an SNMP Get. The MIB file is in the *library* folder and is named *htmMib.mib*. Most installations won't enable this feature and it's not needed in order for Hitachi Remote Ops Monitor Agent to monitor devices. This function is only used for those customers who wish to receive an SNMP trap from Hitachi Remote Ops Monitor Agent in the event the agent detects an issue on a monitored device. It doesn't affect notifications sent to Hitachi Vantara.

The following types of traps will be issued -

- *htmDeviceFail* is sent when a device is put into the 'Device Errors' table (as seen on the Summary display).
- *htmDeviceCommFail* is sent when a device is put into the 'Communication Errors' table (as seen on the Summary display).
- *htmDeviceDisable* is sent when a device is put into the 'Not Monitored' table (as seen on the Summary display).

To configure Hitachi Remote Ops Monitor Agent to send a notification, perform the following configuration steps -

- Set the SNMP Agent parameters in the Configuration->Transport Agents page in the *SNMP Agent Configuration* section.
- Configure at least one Remote NMS (Remote Network Manager System). Multiple NMS locations may be configured by a comma separated list.
- Configure the *Trap Security Name* to the required name - typically 'public'.
- To perform SNMP v2c requests to Hitachi Remote Ops Monitor Agent configure a *Read Security Name*. This is typically set to 'public'.

• **Log Files**

By default, the Hitachi Remote Ops Monitor Agent stores its log files in the installation directory (hds\hitdfmon by default) and this is suitable for most installations but it's possible to change this location by adding the following parameter in the HitDFmon.config file (restart the Hitachi Remote Ops Monitor Agent program after making this change):

LogNameTemplate = prefix The default prefix is HiTrack, Hitachi Remote Ops Monitor Agent will form the log filename from prefixyyyymmdd.log, where yyyymmdd is the current date. Prefix may include a directory path: *LogNameTemplate = dirPath\HiTrack* (use a forward slash for Linux systems) will create log files in the directory dirPath with the filename HiTrackyyyymmdd.log.

• **CR-LF (Carriage Return, Line Feed) characters**

In the unusual case where CR-LF (Carriage Return, Line Feed) characters are defined in the following FTP fields: Host, UserId, Password and Account, the configuration parameter 'escapeCRLF' must be defined in the configuration file HitDFmon.config.



escapeCRLF = CRLF

Note that any text string may be used to define the CR-LF sequence. The defined text string can then be used in the FTP fields (either in the configuration file, or in the HTML configuration pages) to include a CR-LF sequence.

FTPHost = hostname1CRLFhostname2

will send the following text when defining the remote FTP server

hostname1

hostname2

- **Tunnel Proxy**

A Tunnel proxy may be defined by entries in the configuration file (HitDFmon.config). This is intended to be used by sites that create the agent configurations programmatically. The proxy is defined by entering the following before an FtpHost or HttpsHost definition:

FtpSoHost = proxy IP Address

FtpSoPort = proxy Port number

The case used for the parameter name (FTPSoHost/FtpSoPort) is not significant. The case used for the parameter value is significant. The two parameters should be used together and affect all following FtpHost and HttpsHost definitions.

When this proxy definition is used for a FTP or HTTPs proxy, the Configuration->Transport display will show the Host and Port addresses set and will also allow modification from the browser pages.

- **Email Subject Line**

A fixed Subject line for the emails sent by Hitachi Remote Ops Monitor Agent may be defined in the configuration file, HitDFmon.config:

EmailSubject = subject line text for all emails

Routine Running of the Hitachi Remote Ops Monitor Agent

The Hitachi Remote Ops Monitor Agent program should be running 24/7 to ensure that it will detect error conditions on the monitored devices and so that it can report to the Hitachi Remote Ops center at Hitachi Vantara on a daily basis. Normally the program runs in the background (as a Windows Service or Linux process) and no window is presented for the program. All interaction with the program is performed via web browser access to the monitor program. Through the browser interface one may set basic configuration items, add new devices, or modify or delete existing devices to monitor, view the status of each device, or view details of a device. A web browser anywhere on the customer's network that has TCP/IP connectivity to the host platform running the Hitachi Remote Ops Monitor Agent can typically be used to interact with the program. It's possible to have multiple browsers from multiple locations access the Hitachi Remote Ops Monitor Agent concurrently. The browser access has two operational levels based on the type of login used - Administrator and Monitor. The Administrator type is allowed to set or change basic configuration items and add/edit/delete devices to monitor. The Monitor type is not allowed to set or change program configuration items but can monitor device status and view device details. When a browser is displaying the device summary page, the page will update itself about every 60 seconds.

The top table on the device summary page displays a summary of the numbers of devices that are presently in a particular monitor category which includes devices exhibiting errors, devices that the monitor program is unable to



communicate with, devices that are reporting okay and with no errors, devices not monitored due to user setting, and total devices configured for the monitor. The table contains checkboxes which determine what categories will be displayed in the tables that follow this summary table. The default is that all tables will be displayed (checkboxes checked).

Up to four tables will follow the summary table. The following tables are presented if any devices exist in the category:

- **Device Error** - This table displays devices which are exhibiting errors. The Status column will be red with a short summary of the error type.
- **Communication Error** - This table displays devices which the monitor program is unable to communicate with. The Status column will be in yellow. The communication error may be due to a network problem, ip address setup problem, or the device is powered off.
- **Device Okay** - This table displays devices that are reporting normally and exhibit no errors. The Status column will be green.
- **Not Monitored** - This table displays devices that the user specified to not monitor even though they're configured in the monitor. This is performed via a checkbox on the item setup. The Status column will be pale yellow. This option may be used to disable checking of the device when maintenance is being performed to the device or when a customer has the device temporarily unavailable.

In each of these four tables the following columns are presented:

- **Item** - Indicates the item number for the device according to the order in which the devices were entered. In administrator mode, the item number is hyperlinked and may be clicked to modify the device's monitor setup parameters and the Item heading is hyperlinked to allow for adding new devices when clicked. Note - It may take a few minutes for the data for a newly added device to be obtained before having valid detail data for the device.
- **Name, Location, Group** - Indicates the name, location, or group set when the device was added. This is for user reference only.
- **Type** - Indicates the type of device (DF Storage, Cisco, etc.).
- **Model** - Indicates the model number of the device (HUS, AMS, etc.).
- **Serial** - Indicates the serial number of the device.
- **Status** - Indicates the error status of the device.
- **Last Communication** - Timestamp of the last time the monitor attempted to communicate with the device. This field is normally updated every few minutes.
- **Site ID** - Indicates the Site ID set for the device at the time it was added.
- **IP Address 1 or 2** - Indicates the IP addresses that were set for the device when it was added.

In the *Status* column for a particular device, the 'D' icon may be clicked to display a page showing details of the device. The detail page includes a number of tables showing error status and configuration details for various functional components including drives, cache, power, fans, microcode levels, etc.

The Hitachi Remote Ops Monitor Agent will send device data related to error and device configuration to the Hitachi Remote Ops center when an error condition is detected and also on a daily basis.

Clicking the *Transport History* navigation button will present a page indicating the data transport activity of the Hitachi Remote Ops Monitor Agent. This can be useful for troubleshooting transport problems. This page also has a *Request Report* button at the bottom which will force a data transport to take place. This can be used to ensure the Hitachi



Remote Ops Monitor Agent is configured properly to transport the data to the Hitachi Remote Ops Center.

Note: For some program configuration changes, the program will indicate to restart the agent. This is done by stopping then starting the "Hitachi Remote Ops Monitor Agent" service through the Windows Control Panel for Windows systems, or by running "sh rundfmon stop" followed by "sh rundfmon start" for Linux systems.

Before stopping the Hitachi Remote Ops Monitor Agent all polling operations should be stopped by using the **Shutdown** command in the browser interface. This is accessed from the *About* tab, the *SHUTDOWN* option in the left hand menu, and finally by clicking the *Confirm Shutdown* button. This command stops all polling and reporting operations - the Thread Activity display is shown while the current polling operations complete. The threads that are ending are shown with a yellow background. When the display shows that Shutdown is complete then the Hitachi Remote Ops Monitor Agent service may be stopped. The Hitachi Remote Ops Monitor Agent does not terminate when the Shutdown command completes - the browser interface continues to run until the service is terminated.

Post-Installation Tests and Verification

After Hitachi Remote Ops Monitor Agent is installed and configured it needs to be checked to ensure it can properly transport from the site to Hitachi Vantara and that the site ID is configured correctly and that there are no other issues. The following steps will validate the installation.

1. After configuring the device(s) to be monitored wait about 5 minutes and check the *Summary* page to ensure the 'Status' column indicates the expected condition for the device, i.e. 'Okay' on a green background or 'Error' on a red background indicating the device itself has an error condition (such as a failed drive, power supply, etc.). Other conditions could indicate an inability for Hitachi Remote Ops Monitor Agent to communicate with the device such as a network issue, wrong IP address, wrong credentials, etc. Any communication issues will need to be resolved.
 2. From the Hitachi Remote Ops Monitor Agent user interface click the *Transport History* button to go to the Transport History page and then click the 'Request Report' button at the bottom of the page to trigger a transport to Hitachi Vantara. Check the 'Transport History' table to see if it appears that the transport was successful. It may take a couple of minutes for the final transport status to appear.
-

Uninstalling the Hitachi Remote Ops Monitor Agent

To uninstall the Hitachi Remote Ops Monitor Agent, perform the following:

1. Windows Uninstallation

1. Stop the Hitachi Remote Ops Monitor Agent program, if running, by stopping the "Hitachi Remote Ops Monitor Agent" service through the Windows Control Panel.
2. Select Add/Remove Programs under the Control Panel and remove the Hitachi Remote Ops Monitor Agent program. Note - not all items will be removed but will be removed in the next step.
3. Delete the installation directory (c:\Program Files\hds by default). Empty it from the Recycle Bin if it's now present in the Recycle Bin.

2. Linux Uninstallation

1. Stop the Hitachi Remote Ops Monitor Agent program, if running, by running "sh rundfmon stop" in the installation directory (/usr/hds/hitdfmon by default).
 2. Run "sh UninstallHiTrackMonitor" in the /usr/hds/hitdfmon (by default) directory.
-



3. Delete the 'hds' directory where the Hitachi Remote Ops Monitor Agent was installed.
-

