

Hitachi Remote Ops Service Processor Agent User Guide

****This article is only visible to Service Partners and Employees****

Service Processor Agent User Guide

A User Guide for the **Hitachi Remote Ops Service Processor Agent Version D.8**



Introduction

The Hitachi Remote Ops Service Processor Agent is an application that monitors devices belonging to the enterprise RAID family of Hitachi Vantara storage products. The application collects configuration data and error information from the monitored systems and reports this data to Hitachi Remote Ops via HTTPS. It also enables certain remote operations like dump acquisition or system updates.

This application supports the following Hitachi Vantara storage products:

- VSP 5600, VSP 5500, VSP 5500H, VSP 5200, VSP 5100
- VSP N800, VSP N600, VSP N400, VSP G800, VSP F800, VSP G600, VSP F600, VSP G400, VSP F400, VSP G200, VSP F200
- VSP G1500, VSP F1500, VSP G1000, VSP F1000
- HUS VM
- VSP

Please Note: The Hitachi Remote Ops Service Processor Agent does not support VSP G900, VSP F900, VSP G700, VSP F700, VSP G370, VSP F370, VSP G350, VSP F350, VSP G130, and VSP F130 systems. Install the latest version of the Hitachi Remote Ops Monitor Agent on these products.

Important Terminology

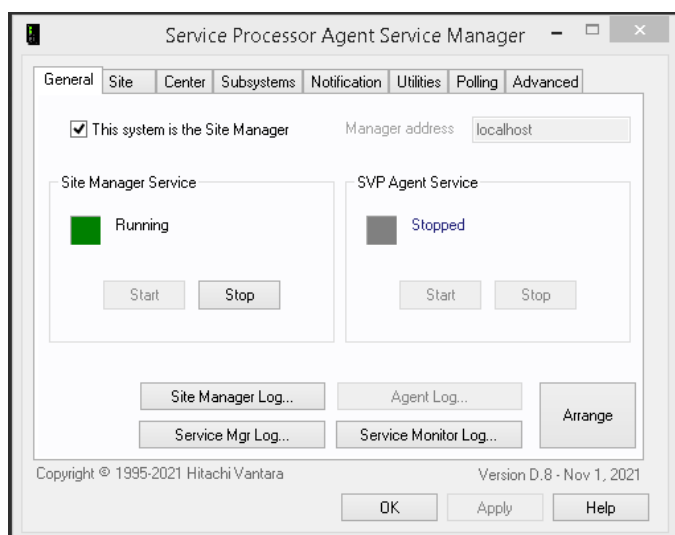
There are five major components to the Service Processor Agent that work in tandem to monitor storage products and communicate with Hitachi Remote Ops.

- **The Service Manager:** This is the interface used to configure the application.
- **The Site Manager:** This service handles communication to both Hitachi Remote Ops and communication to the storage products being monitored. It can be run on either a standalone Windows machine or the service processor (SVP) of one of the monitored storage products.
- **The SVP Agent:** This service monitors the storage product and runs on the SVP of the product.
- **The Service Monitor:** This always-on service monitors the application.
- **The Web Interface:** This service enables and hosts a web interface for remote operations on the device functioning as a Site Manager.

Service Manager

The interface for configuring the application is called the Service Manager (pictured below). It is used to configure, start, and stop the services. The Service Manager runs on all devices that the application is installed on so that you may manage the relevant services on that system. The Service Manager is Windows application that is launched at login. On SVPs, the system automatically logs in the Administrator account at startup, so the Service Manager will launch at startup.





Site Manager

The Site Manager service coordinates communication between Hitachi Remote Ops and the storage products that it manages. This service can be run on an SVP or on a different computer altogether.

With a customer installation that consists of multiple storage products, most often, one system will be configured as a Site Manager, while also running the SVP Agent on itself, and the others will be configured to only run the SVP Agent. For example, a customer site with three systems may be configured as follows:

Subsystem	Services Running
Subsystem 1 (VSP)	Site Manager SVP Agent (back 00)
Subsystem 2 (VSP G1000)	SVP Agent (back 01)
Subsystem 3 (HUS VM)	SVP Agent (back 02)

If a customer installation consists of a single system, that system can be configured to both run the SVP Agent and function as its own Site Manager.

SVP Agent

The SVP Agent service will regularly monitor a system for new errors and collate configuration and performance data. This component will also apply remote operations received from either Hitachi Remote Ops or from the Web Interface, e.g dump generation or applying a system update.

Web Interface

This service allows users without direct login access to an SVP functioning as a Site Manager or to a standalone Site



Manager to request that a Site Manager generate and transfer an dump to Hitachi Remote Ops for one or more systems. User access to the Web Interface is administered within the Web Interface.

To use this feature, the feature must be enabled within the Service Manager on the Site Manager and the service must be running. When enabled, the port that was configured during installation is opened by the service and firewall rules are added to allow incoming traffic. The Web Interface can be accessed either from the start menu on a Site Manager or via URL. The URL format will be **https://IP:PORT/** where *IP* is the Site Manager's internet or intranet IP address and *PORT* is the number of port that was configured during installation. The default port value is 4431.



Installation

Planning Deployment

Before beginning the installation procedure, you will need to plan and ensure that you have the information you'll need to fully configure a site.

Identify the computer system that will function as the Site Manager. This may be a storage product or it may be a separate computer system. The Site Manager serves as the communication channel between the Hitachi Remote Ops and all of the systems at a customer site.

At customer sites equipped with only a single storage product, it is common to configure that system with both a Site Manager and an SVP Agent. This means that the system will need to have HTTPS access to the internet in order to communicate with Hitachi Remote Ops.

Important note: There must be one, and may only be one, Site Manager for a group of one or more systems that are networked together. Using redundant Site Managers to monitor a system or a group of systems is not supported by Hitachi Remote Ops.

Preparation

Before beginning any software installation, prepare notes including:

- The serial numbers and IP addresses of each system to be managed by the Site Manager
- The IP address or hostname of the Site Manager

Operating System Requirements

The application supports installation on the following versions of the Windows OS:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2
- Windows 11
- Windows 10
- Windows 8.1



- Windows 8
- Windows 7 SP1
- Windows Vista SP2

Site Manager Requirements

The Site Manager needs:

- TCP/IP connectivity to the SVP of each system monitored by the Site Manager
- Outbound HTTPS access on port **443** for transferring data
- The following ports open*: **2056** and **2057**

SVP Agent Requirements

The SVP Agents need:

- TCP/IP connectivity to the Site Manager
- The following ports open*: **2056** and **2057**

Web Interface Requirements

The Web Interface needs:

- The IP address or hostname of the Site Manager
- An alternate port to use for the Web Interface if the default port of **4431** is already in use
- The chosen port must be open between the host and the Web Interface's users
- A customer supplied SSL certificate if the added security is desired
 - The application will otherwise install and attach a self-signed SSL certificate to the Web Interface

To open ports: Use Windows Firewall to check or set port settings.



Notes on Upgrading from Prior Versions

There are a few important changes to functionality you should be mindful of when upgrading from prior versions of the application.

Versions D.7 and lower are not compatible with versions D.8 and higher of the application. When upgrading the application at a site, the best practice is to upgrade the application on both the Site Manager and on all the systems that it is monitoring to the latest version.

FTP and FTPS contact methods were deprecated in version D.7. Upgrading the application will remove any previously defined FTP and FTPS methods from the application's configuration.

Default HTTPS contact methods for transport to Remote Ops will be defined where any are missing. The default polling servers for Remote Ops requests will be added where missing as well. We encourage you to ensure that the site is able to reach all defined HTTPS transport locations and able to poll all defined poll servers when you configure the application.



Deploying the Application

Follow these recommendations to ease the process of deploying the Service Processor Agent in a single or multiple system environment.

Network IP Address

Generally, we recommend that you use the system's private LAN addresses where possible. This will reduce the likelihood of complications from the customer's switches, routers, gateways, etc. By using the private LAN, you will also avoid competition for network bandwidth on the customer's public LAN.

However, public LAN settings may also be used to connect a Site Manager to an SVP Agent, if preferred.

Whether you're using private or public LAN, ensure that you have TCP/IP connectivity between the Site Manager and all SVP Agents. In addition, TCP/IP packets addressed to certain ports must be able to transit the customer network. See the [Planning Deployment](#) section for the ports used for intersystem communications.

Installation Order

The quickest way to deploy the application at a site with multiple subsystems is to [Install the Application](#) on the Site Manager first.

[Configure the Site Manager](#) and then start the Site Manager service. If the Site Manager is running on a storage product, [Configure the SVP Agent](#), and then start the SVP Agent after you've started the Site Manager. The SVP Agent will register the storage product with the Site Manager when you start the SVP Agent.

Next, go to each other storage product, one by one, and install and [Configure the SVP Agent](#) on the SVP of that system. If the system is utilizing Dual SVPs, follow the notes about [Deploying on Dual SVPs](#).

You will need to provide the address for the Site Manager system to each of the SVP Agents as you configure them. After you install the software and specify the address of the Site Manager, open the SVP Agent log, which will initially be empty. Then, apply your settings and start the services. Watch the startup messages in the log. If the Site Manager service is running, you should see a log message indicating that the SVP Agent registered with the Site Manager.

When you have finished configuring the each of the SVP Agents, return to the Site Manager and bring up the Service Manager. Click on the **Subsystems** tab and look at the list of systems under management. You should see an entry in the list for each SVP Agent that you configured on a storage product.

You can open the Site Manager log to monitor the Site Manager's functions. You can also open the SVP Agent logs from the Site Manager by clicking the **Subsystems** tab in the Service Manager and then clicking the **View Log** button in the **Subsystem Properties** window for each system. To neatly arrange the log windows, go back to the **General** tab and click the **Arrange** button.



Once the site has been configured, navigate to the **Utilities** tab. To test data collection and transfer of data to Hitachi Remote Ops by checking the **Generate new data files** option and clicking **Transfer Now**. If this is a new installation of the application and the **Generate new data files** option is not checked, there will be no data files to collect and send. The SVP Agent logs will detail the progress of the data collection and the Site Manager logs will detail the progress of the transfer to Hitachi Vantara once all systems have completed their data collection.

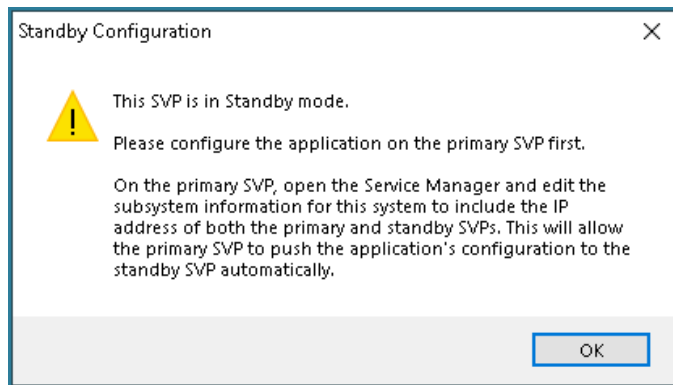


Deploying on Dual SVPs

On systems equipped with dual SVPs, the application must be installed on both the primary and standby SVP in order to fully take advantage of the dual SVPs' intended redundancy.

Install the application on the standby SVP first and then start the SVP Agent without configuring the application. The standby SVP will be configured by the primary SVP once you have configured the SVP Agent on the primary SVP. You will be warned by the application to configure the primary SVP first, once you've installed the application on the standby SVP.

Note that the Site Manager service will be disabled on standby SVPs. Site Manager functionality is not supported on standby SVPs, but in the event of the standby SVP becoming the primary SVP, the Site Manager functionality will be enabled and will run with the settings that were configured for the Site Manager on the prior primary SVP before the switch.



Next, install the application and configure the primary SVP. If the application has been configured to either point towards a remote Site Manager or the application has been configured to run as its own Site Manager, the SVP Agent service can then be started.

Navigate to the **Subsystems** tab. Double-click on the system to open up the **Subsystem Properties** for it. This window will already be populated with information about the standby SVP if the the primary and standby SVPs are using one of the IP address conventions that are recommended in the maintenance manuals for the storage product.



Subsystem Properties

IP address or host name: localhost

Registration Address (reachable from Site Manager)

Primary SVP IP Address (reachable from Standby)

Standby SVP IP Address (reachable from Primary) 126.255.254.14

System Properties

Type: VSP 5200/5600

Serial number: 40016

DKC: 90-08-00-00/12

SVP: 90-08-00-12/15

Options

☒ Allow FC-GS queries

☒ Gather Config.zip

View Log Generate Dump File

Generate Data Files Transfer Dump Files

Close

If not, you will need to populate the **Standby SVP IP Address** field with the IP address of the standby SVP that is reachable from the primary SVP and then populate the **Primary SVP IP Address** field with the IP address of the primary SVP that is reachable from the standby SVP. Likewise, if you would prefer the primary and standby SVPs use different IP addresses for connecting to each other than those that have been pre-populated into the aforementioned fields, you may change these settings to use the preferred IP addresses.

Subsystem Properties

IP address or host name: localhost

Registration Address (reachable from Site Manager)

Primary SVP IP Address (reachable from Standby) 10.1.1.1

Standby SVP IP Address (reachable from Primary) 10.1.1.2

System Properties

Type: VSP 5200/5600

Serial number: 40016

DKC: 90-08-00-00/12

SVP: 90-08-00-12/15

Options

☒ Allow FC-GS queries

☒ Gather Config.zip

View Log Generate Dump File

Generate Data Files Transfer Dump Files

OK Cancel

As you first configure the SVP Agent on the primary SVP, you may be warned that the SVP Agent is unable to connect to the standby SVP if the SVP Agent service has not yet been started on the standby SVP. However, once the SVP Agent has been started on the standby SVP, the SVP Agent on the primary SVP will automatically mirror the application's settings to the standby SVP, correctly configuring the SVP Agent on that SVP.

Service Manager

⌵

⚠ SVP Agent was not able to update the standby SVP. Ensure that Service Processor Agent is installed and running on both the primary and the standby.

OK



After you have installed and configured the Service Processor Agent on the dual SVPs, you only need to make configuration changes on the primary. Whenever you change the application's settings on the primary and click **OK** or **Apply**, the Service Processor Agent will automatically migrate the new settings to the standby, so long as the SVP Agent service is running on the standby SVP. If the SVP Agent service is not running, the new settings will migrate as soon as the SVP Agent service resumes running on the standby SVP.

Testing Deployment on Dual SVPs

To fully test the application on dual SVPs, perform an SVP swap.

After a few minutes you can reestablish your Remote Desktop session to the new primary SVP. Use the Service Manager to view the logs and verify that the former standby SVP was in standby mode and switched to primary mode. Similarly RDP to the new standby SVP and verify through the logs that the SVP was in primary mode and then registered that it was in standby mode.

If you perform this test, don't forget to perform a swap again to return the actual primary SVP to primary mode. And finally, wait for the swap to complete and ensure that the Service Manager comes up again properly on the new (original) primary SVP.



Installation Overview

To install the application from a CD:

- Insert the Service Processor Agent CD-ROM into the machine
- Log onto the SVP or the standalone Windows device
- Open Windows Explorer
- Navigate to and open the CD drive
- Double-click **autorun.hta**
- Follow the installer prompts

To install the application on an SVP remotely:

- If installing from a CD, insert the CD and open up the CD drive in Windows Explorer. If installing from downloaded installation media, unzip the compressed installation media and open that location within Windows Explorer
- Launch Remote Desktop
- In the **Computer** box, enter the IP address of the SVP
- Click the **Options>>** button to expand the Options dialog
- Enter the credentials for the administrative account within the user name and password fields
- Click the **Local** Resource tab
- In the **Local devices** group box, check the **Disk Drives** option
- Click the **Connect** button
- On the SVP:
 - Open Windows Explorer and copy the installation media from your local machine to the SVP
 - Double-click **autorun.hta**
 - Follow the installer prompts

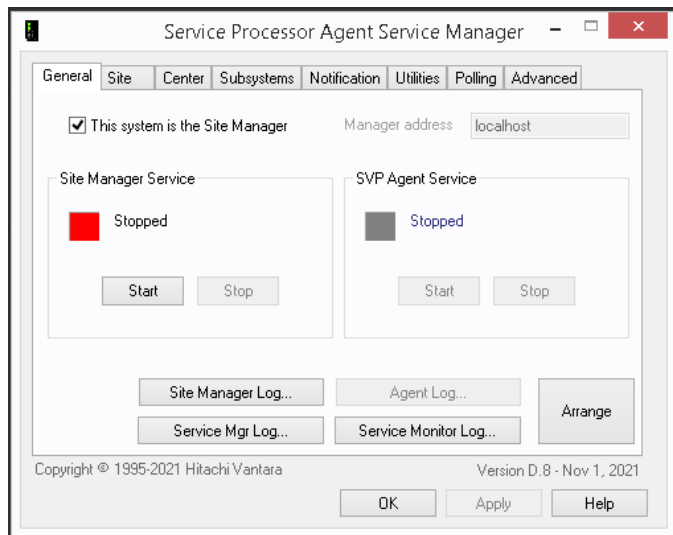
During installation, prerequisite software may be installed if it is not already installed on the system. For this reason, the installation may take a variable amount of time to complete. You may also be prompted to reboot the SVP after installing one of the components. If so, reboot the SVP and begin the installation process again, which will skip over the already installed prerequisites.

See [Planning Deployment](#) for a list of prerequisite software.

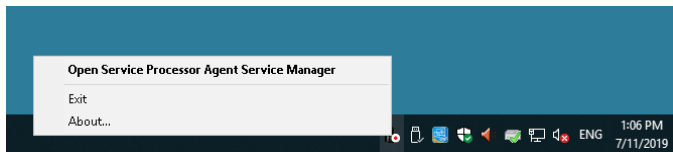


Configuring the Application

After the installation, you will be given an option to **Launch** the **Service Manager** (pictured below).



You should also see a new icon in the system tray that can be used to similarly open the Service Manager. If the icon is missing or you previously exited the Service Manager, you can navigate to the Service Manager from the Start Menu. It will be found within the Hitachi Vantara directory.



Don't click any buttons yet. If you click **OK** (or **Apply**) the Service Manager will validate the settings you have entered, but if you have freshly installed this application for the first time, you won't have entered any setting yet.

Follow the guidelines in [Deploying the Application](#) to customize the installation and then click **OK**.

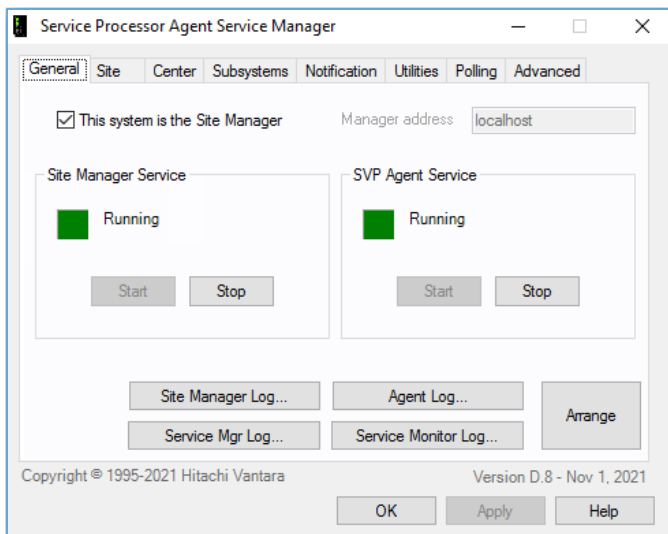


Configuring a Site Manager

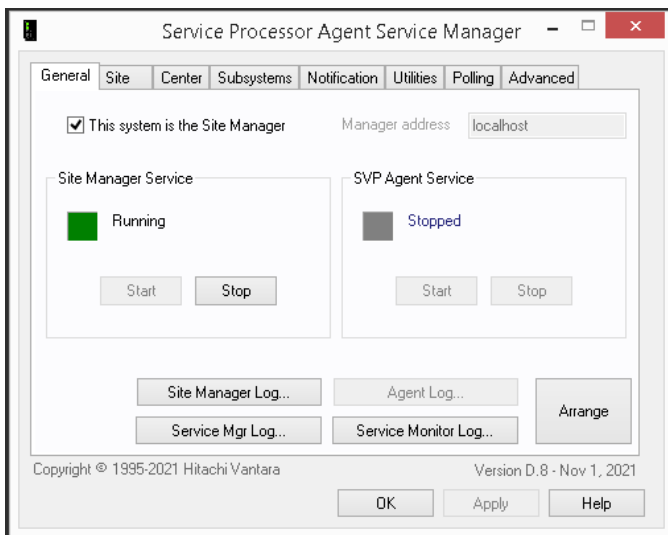
The Site Manager is the device that communicates with Hitachi Remote Ops.

The General Tab

To configure a Service Processor Agent installation as a standalone Site Manager, open the Service Manager and check the **This system is the Site Manager** option on the **General** tab.

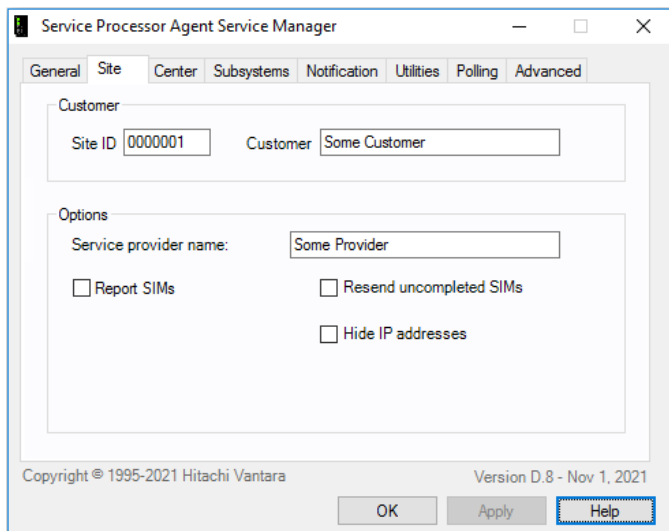


If the Site Manager is running on a standalone computer that is not an SVP, the SVP Agent service will be disabled in the Service Manager.



The Site Tab

Click the **Site** tab and enter the pre-assigned site ID for this customer in the **Site ID** field. Enter the customer's organization name in the **Customer** field.



The screenshot shows the 'Service Processor Agent Service Manager' window with the 'Site' tab selected. The 'Customer' section contains a 'Site ID' field with the value '0000001' and a 'Customer' field with the value 'Some Customer'. The 'Options' section includes a 'Service provider name' field with the value 'Some Provider' and three checkboxes: 'Report SIMs', 'Resend uncompleted SIMs', and 'Hide IP addresses', all of which are currently unchecked. At the bottom, there are 'OK', 'Apply', and 'Help' buttons. The footer text reads 'Copyright © 1995-2021 Hitachi Vantara' and 'Version D.8 - Nov 1, 2021'.

Enter the name of the service provider in the **Service provider name** field. On new installations, the **Service provider name** will default to "Hitachi Vantara". The value you enter for this field will be used in the email notifications from the Site Manager, allowing the email notifications to be customized to the provider. Partner service providers may prefer that their company name is displayed.

Check **Report SIMs** if the Site Manager should report SIM messages to Hitachi Remote Ops.

Check **Hide IP addresses** if you do not want to mask the IP addresses of the SVP Agents being monitored.

Check **Resend uncompleted SIMs** if the Site Manager should perform a daily check for any and all SIMs that have not been marked completed in the SVP and resend those SIMs to Hitachi Remote Ops. This option will continue to resend SIMs until they are marked complete. Do not check this checkbox unless you want a daily reminder to resolve and complete SIM messages.

The Center Tab

Follow the directions in [Configuring the Center Tab](#) to populate the controls in this tab.

The Subsystems Tab

Follow the directions in [Configuring the Subsystems Tab](#) to populate the controls in this tab.

The Notifications Tab

Follow the directions in [Configuring the Notifications Tab](#) to populate the controls in this tab.



The Polling Tab

Follow the directions in [Configuring the Polling Tab](#) to populate the controls in this tab.

Finalizing Site Manager Configuration

Follow the directions in [Finalizing the Configuration](#) to finish configuring the Site Manager.



Configuring an SVP Agent

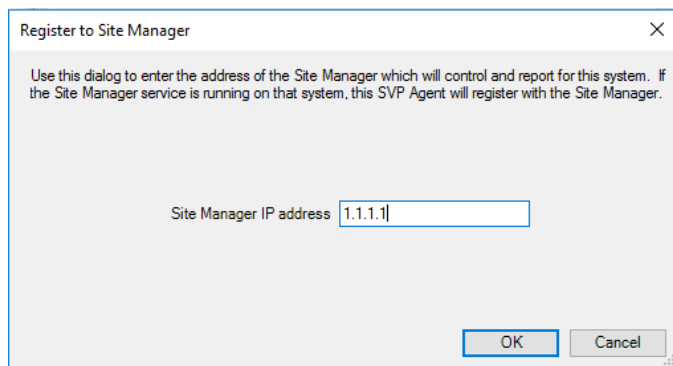
Open the Service Manager on the SVP of the storage product that you would like to monitor. Navigate to the **General** tab.

Configuring the SVP to be a Site Manager

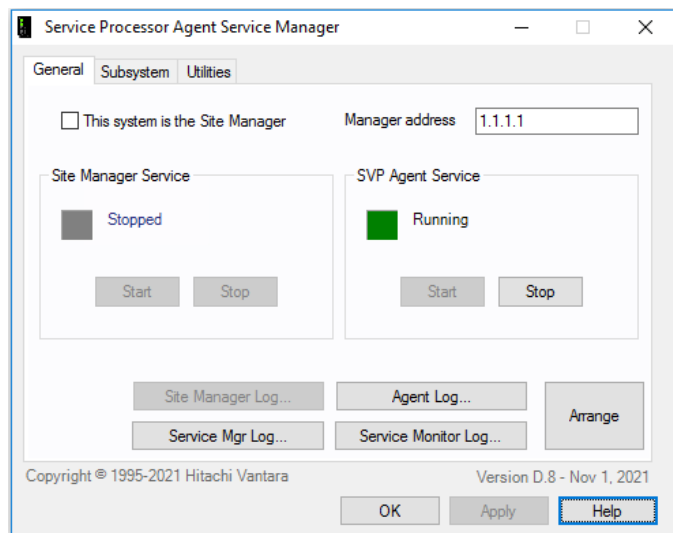
If the Site Manager service should run on this SVP, follow the directions in [Configuring a Site Manager](#) to configure the Site Manager.

Configuring the a remote Site Manager

If the SVP Agent should report to a remote Site Manager, uncheck the **This system is Site Manager** option. When you deselect this option, you will be presented with a dialog box like the one below. Enter the IPv4 or IPv6 of the Site Manager and click **OK**.



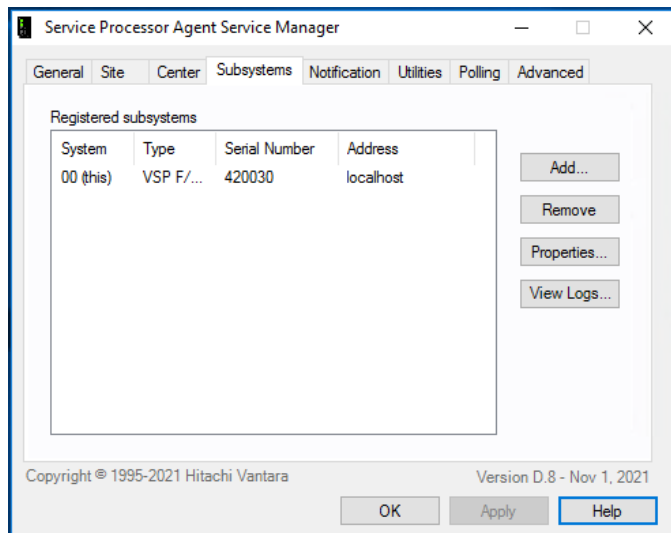
Once you've finished, the Site Manager service will be disabled.



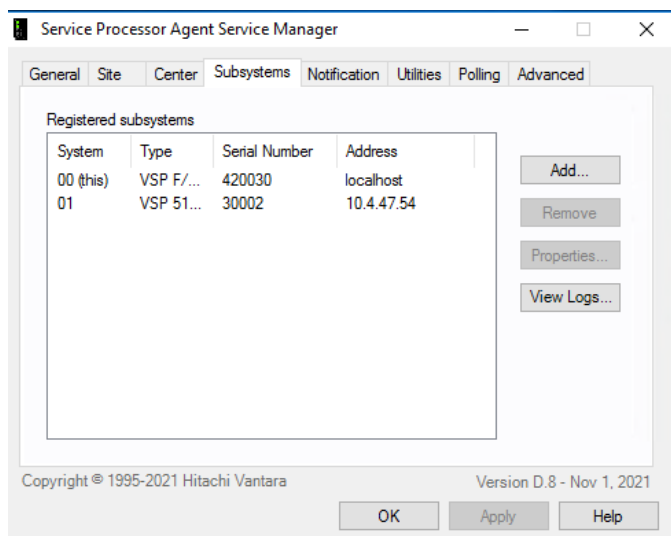
Configuring the System

Click the **Subsystem** tab.

If the SVP is only running an SVP Agent, this tab will only contain the definition for the system this SVP belongs to.



If the SVP is also running a Site Manager, this tab may already display a list of systems managed by the Site Manager if the other SVP Agents meant to be monitored have already been configured.



Auto-Configured Systems

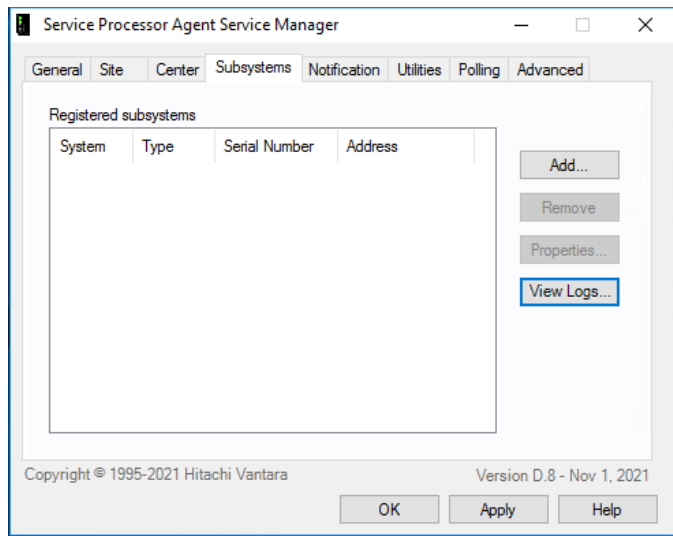
The system in the **Subsystems** listing that correlates to the current SVP will have the word **this** within parentheses.

If the Service Manager was able to communicate with the SVP at the time it was first run, the system properties will already be populated with the storage product model and the serial number. The **IP address** of the system will also be set to the default IP address "localhost".

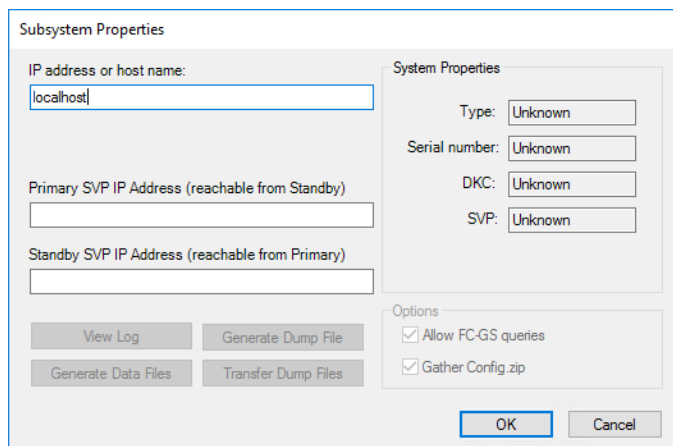


Manually Configured Systems

If the Service Manager has not added an entry in **Subsystems** for the current SVP, click **Add**.



This will bring up a Subsystem Properties window. Enter "localhost" within the **IP address** field and then click **OK**.



The newly defined system should be auto-populated with its identifying information if the SVP services are running normally on the SVP.

Choosing a Registration Address

If the Site Manager is not configured to run on the SVP, the system can be further configured from the **Properties** menu to define an explicit IP address to use when registering with a remote Site Manager. For systems that have multiple IP addresses locally configured, this allows you to choose the IP address that you would like the Site Manager to register. It should be an IP address for the SVP that is reachable from the Site Manager.

Enter this address within the **Registration Address** field. If the OS supports IPv6 and IPv6 is being used for the registration address, the IPv6 address should be wrapped in square brackets and the scope ID (denoted by the '%')



should be omitted.

If this setting is omitted the application will make a best guess as to which of the SVP's interfaces should be used to register with the remote Site Manager. This guess may be inaccurate if the Site Manager is on a different subnet from the SVP Agent.

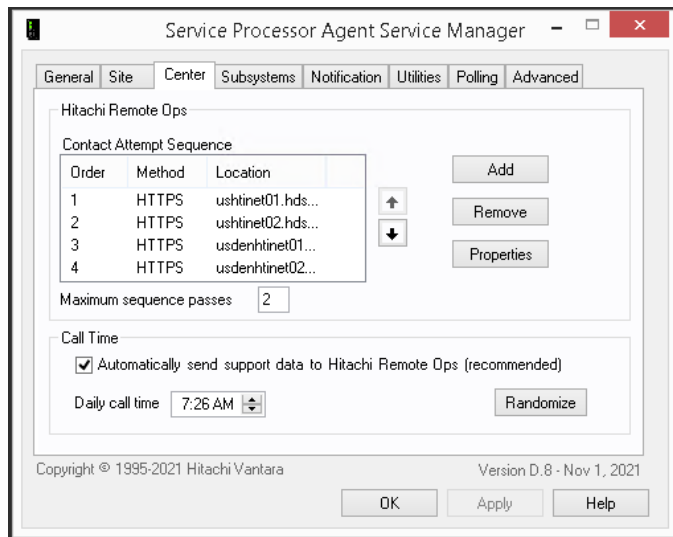
When the Site Manager is configured to run on the SVP itself, the Registration Address setting is not available. The SVP Agent for the local system defined at **localhost** will be reachable from the locally running Site Manager.

Finishing the SVP Agent Configuration

Follow the directions in [Finalizing the Configuration](#) to finish configuring the SVP Agent.



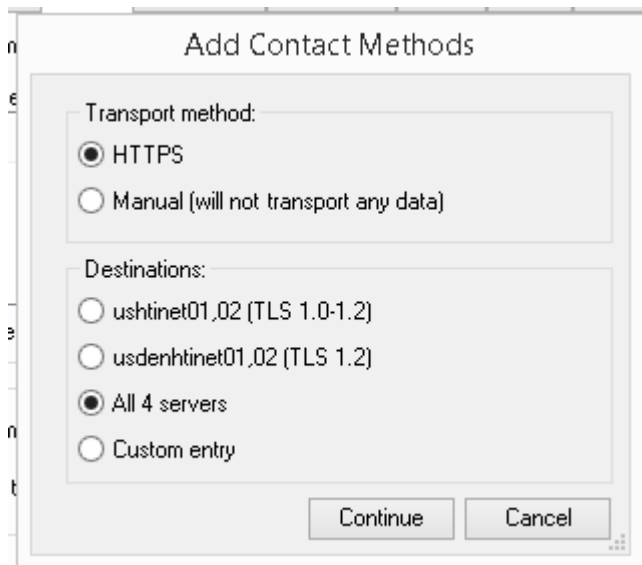
Configuring the Center Tab



This tab lists the Hitachi Remote Ops destinations that the Site Manager will send Service Processor Agent data to within the **Contact Attempt Sequence** control. Multiple HTTPS destinations are defined by default so that the application can failover to another option if a particular HTTPS connection cannot be established successfully.

Adding Contact Methods

To add a contact method, click the **Add** button from the **Center** tab of the Service Manager. This will open the **Add Contact Methods** dialog.



This dialog can be used to add all failover Hitachi Remote Ops destinations with the needed information already pre-populated. We suggest selecting the **All 4 servers** option.



On SVPs running older versions of Windows like Windows Vista or Windows Server 2008, TLS 1.2 is not natively supported. In this case, the Site Manager will not be able to transfer to the two destinations that strictly require TLS.1.2. Using the **ushtinet01,02** option should suffice for failover purposes in this circumstance.

The Custom entry can be used to add an HTTPS destination beyond the four official Hitachi Remote Ops destinations, in the event that function is needed.

Once you've selected the contact method(s) you want to add, click **Continue**.

Manual Transport

It is also possible to configure a **Manual** transport method that will prevent the application from transporting of data to Hitachi Remote Ops. The Site Manager will still collect data from the SVP Agents, but the data collected will remain stored within the **C:\HDS** directory and will not transport to Hitachi Remote Ops.

The **Manual** transport method is only meant to be used at customer sites that do not support a direct internet connection to Hitachi Remote Ops. Using the Manual method, field engineers can copy the files into a different computer and transfer them from there to the Hitachi Remote Ops.

Note that you will need to remove any other existing contact methods before adding a **Manual** method. Likewise, you won't be able to add HTTPS contact methods if a **Manual** method is still defined.

Deprecated Contact Method Types

Deprecated contact method types will be removed from the configuration when upgrading from prior versions of the application. FTP, FTPS, and Dial-Up contact methods are no longer supported by the Service Processor Agent.

Editing an HTTPS Contact Method

An HTTPS contact method requires, at a minimum, an address, a username, and a password. At some customer sites, you may also need to define the proxy server attributes to get HTTPS transfers working properly. Refer to the



[Configuring Proxies on Contact Methods](#) section if the customer site requires internet traffic to pass through a proxy.

The **Validate Server Certificate** option will make sure that the HTTPS certificate validates properly.

The **Times to attempt** option controls how many times a Site Manager will attempt to use and retry the contact method in transfer attempts that do not succeed. The default value is 4. .

The **Test** button allows you to test transferring to the defined destination if the Site Manager service is running. If the Site Manager service is not running, the **Test** button will be disabled. You can view the progress of the test call within the Site Manager log.

Controlling Transfer to Hitachi Remote Ops

The **Maximum sequence passes** control allows you to adjust how persistent the Site Manager will be in contacting Hitachi Remote Ops before failing completely. Specifically, this option controls the number of times the Site Manager will attempt to loop through the list of configured contact methods before exhausting its attempts to transfer to Hitachi Remote Ops. You can select any value between 1 and 99. The default value for this option is 4, which means the Site Manager will make four complete passes through the contact method list before giving up.

Note that the application will defer to the lowest setting between the **Maximum sequence passes** and a contact methods **Times to attempt** setting.

Contact methods will also be attempted in a random order for every transfer. When multiple contact methods are defined, no one method is going to be treated as preferred.

Configuring Daily Transfer to Hitachi Remote Ops

We recommend that you leave the **Automatically send support data to Hitachi Vantara** option checked. This ensures that the application will generate configuration data on a daily basis and send it to Hitachi Remote Ops.

The difference between disabling this option and using a Manual contact method is that SIM data will continue to be transfer to Hitachi Remote Ops even if the **Automatically send support data to Hitachi Vantara** option is deselected, as long as a valid contact method is defined.

The **Daily call time** option allows you to set when the Site Manager will begin the daily call process. You can randomize this setting by clicking the **Randomize** button. There is no set default for this setting. The Service Manager will randomize this setting when it starts up for the first time.

We recommend that you leave the call time at its default random value to help normalize the times that sites call into the Hitachi Remote Ops.



Configuring Proxies on Contact Methods

A Site Manager can be configured to use several types of proxy servers for an HTTPS Contact Methods:

- HTTP Proxy
- SOCKS4 Proxy
- SOCKS5 Proxy

To configure a proxy, open the Service Manager and navigate to the **Center** tab. For each destination that requires a proxy to be configured, double-click the contact method or select the contact method and click **Properties**. In the HTTPS Method Properties window, you can select the type of proxy that needs to be configured with the **Type** option.

The screenshot shows the 'HTTPS Method Properties' dialog box. The 'Properties' section includes 'Times to attempt' (4) and 'Validate Server Certificate' (unchecked). The 'Address' is 'ushinet02.hds.com' and 'Port' is '443'. The 'Username' is 'ht_http_test' and the 'Password' is masked with a checkbox for 'Hide password'. The 'Proxy server' section has a 'Type' dropdown menu with options: None, HTTP, SOCKS4, and SOCKS5. The 'Proxy authentication' section includes 'Username', 'Password', and 'Domain' fields, and a 'Use Digest Authentication' checkbox. At the bottom are 'Test', 'OK', and 'Cancel' buttons.

HTTP Proxies

HTTP proxies expect to send and receive HTTP web requests from the Site Manager. For clients equipped with HTTP proxies, enter the address and port of the proxy, as well as any authentication information that needs to be configured.



HTTPS Method Properties

Properties

Times to attempt: 4 (0 = disabled) ☒ Validate Server Certificate

Address: ushtinet01.hds.com Port: 443

Username: ht_http_row Password: ☒ Hide password

Proxy server (for all HTTPS methods and polling)

Type: HTTP Address: 1.1.1.1 Port: 8080

Proxy authentication (optional)

Username: Password:

☐ Use Digest Authentication Domain:

Test OK Cancel

SOCKS Proxy Servers

To configure a SOCKS proxy, select SOCKS4 or SOCKS5 as appropriate from the Type settings. Then configure the address and port of the proxy, the IP address of the local interface that should be used to communicate with the proxy, and any authentication information needed.

HTTPS Method Properties

Properties

Times to attempt: 4 (0 = disabled) ☒ Validate Server Certificate

Address: ushtinet01.hds.com Port: 443

Username: ht_http_row Password: ☒ Hide password

Proxy server (for all HTTPS methods and polling)

Type: SOCKS4 Interface IP: Address: 1.1.1.1 Port: 8080

Proxy authentication (optional)

Username: Password:

☐ Use Digest Authentication Domain:

Test OK Cancel

Please note that issues with legacy SOCKS proxy servers can be difficult to troubleshoot.

Troubleshooting

When troubleshooting proxy connection issues, you may need to work with the customer's IT staff. You may also need to use tools to capture TCP/IP packets and analyze them to determine the nature of the problem.

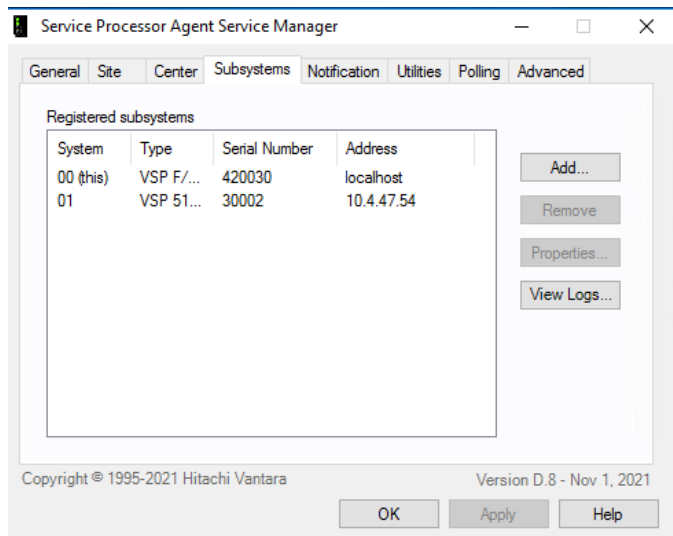


Configuring the Subsystems Tab

Refer to the [Configuring an SVP Agent](#) section when configuring the local system to be monitored by an SVP Agent.

Configuring Subsystems on the Site Manager

Open the Service Manager on the Site Manager and navigate to the **Subsystems** tab. This panel displays the list of systems being managed by this Site Manager.



If the SVP Agent has already been installed and configured on a system that should be reporting to this Site Manager, the SVP Agent will automatically register with the Site Manager once the Site Manager service is running and the system being monitored by that SVP Agent will show up within the list of **Registered subsystems**. The easiest way to configure a site is to:

1. Configure the Site Manager
2. If the Site Manager is running on an SVP, configure the SVP Agent on that SVP
3. Install and configure the SVP Agent on the SVP of each storage product that should be monitored by the Site Manager

Manually Adding Systems

To manually add a system that is not already being monitored by the Site Manager, click **Add**. This brings up the **Subsystem Properties** dialog box.



Subsystem Properties

IP address or host name:

Options:

- ☒ Allow FC-GS queries
- ☒ Gather Config.zip

View Log

Generate Data Files

Generate Dump File

Transfer Dump Files...

System Properties:

Type:

Serial number:

DKC:

SVP:

OK Cancel

Type in the IP address of the system you are adding and click **OK**. If the system is configured with multiple IP addresses, choose the IP address that is reachable from the Site Manager.

When you return to the **Subsystems** tab, you will see your new entry in the list of subsystems. If the Service Processor Agent is already installed and the SVP Agent is running on this system, the Site Manager will automatically populate the **Subsystem Properties** of this newly defined system. If the SVP Agent is not already installed or is not running, the **Subsystem Properties** will display as "Unknown" until communication has been established between the Site Manager and the SVP Agent on the system.

Subsystem Properties

IP address or host name:

Options:

- ☒ Allow FC-GS queries
- ☒ Gather Config.zip

View Log

Generate Data Files

Generate Dump File

Transfer Dump Files...

System Properties:

Type:

Serial number:

DKC:

SVP:

Close

You can view a system's Subsystem Properties by double-clicking the system or by selecting the system and clicking **Properties**.

Editing and Collecting Data From a System

The **Allow FC-GS queries** setting is enabled by default. During daily call, three of the configuration files generated gather FC-GS information from the SVP microcode by performing an industry standard FC-GS RNID query to attached host HBAs and switches. Under certain hardware/driver combinations, this query could result in problems with attached hosts or switches. If this setting is enabled, the SVP Agent will generate these data files. Disabling this setting will cause



the SVP Agent to skip generating these files.

The **View Log** button allows you to remotely view the SVP Agent log of the system.

The **Generate Data Files** button allows you to trigger fresh collection of configuration data from that system.

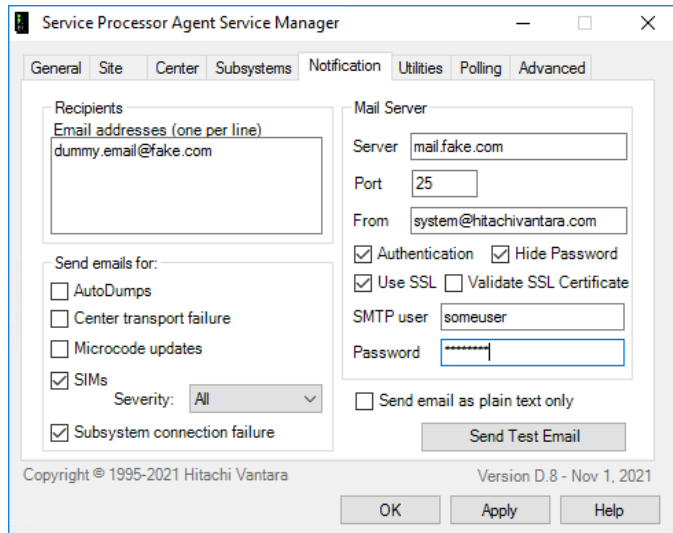
The **Generate Dump File** button allows you to generate and transfer a dump from that system to Hitachi Remote Ops.

The **Transfer Dump Files** button allows you to select an existing SVP dump from that system and transfer it to Hitachi Remote Ops.



Configuring the Notifications Tab

In the Service Manager, click the **Notification** tab. These settings enable the application to send email alerts to the customer if the Site Manager or monitored systems exhibit certain problems, and allow the customer to also be alerted when dumps are collected or system updates are performed.



The screenshot shows the 'Service Processor Agent Service Manager' window with the 'Notification' tab selected. The window contains several configuration sections:

- Recipients:** A text area labeled 'Email addresses (one per line)' containing 'dummy.email@fake.com'.
- Send emails for:** A list of checkboxes: 'AutoDumps' (unchecked), 'Center transport failure' (unchecked), 'Microcode updates' (unchecked), 'SIMs' (checked), and 'Subsystem connection failure' (checked). A 'Severity' dropdown menu is set to 'All'.
- Mail Server:** Fields for 'Server' (mail.fake.com), 'Port' (25), and 'From' (system@hitachivantara.com). Checkboxes for 'Authentication' (checked), 'Hide Password' (checked), 'Use SSL' (checked), and 'Validate SSL Certificate' (unchecked). Fields for 'SMTP user' (someuser) and 'Password' (masked with asterisks).
- Send email as plain text only:** An unchecked checkbox.
- Buttons:** 'Send Test Email', 'OK', 'Apply', and 'Help'.
- Footer:** Copyright © 1995-2021 Hitachi Vantara, Version D.8 - Nov 1, 2021.

Notes on Use

This feature is not a replacement for daily call home to Hitachi Remote Ops or for call home of SIMs.

Please consider the ramifications of any of these settings before enabling email notifications. For example, if the Site Manager is configured to resend uncompleted SIMs each day and also configured to send email alerts about SIMs, then an email message will also be sent each day to the configured recipients until all SIMs are completed.

If you configure email notifications at the request of a customer, be sure to explain explicitly to them that they do not need to take actions based on email messages they receive. Hitachi Vantara will still be notified of events and cases will be opened in the usual way. If the customer responds to email notifications by opening a separate case with Global Support, this may lead to duplicate cases being opened for the same issue.

You may want to consult with your manager before enabling this feature.

Types of Notifications

There are five events that can cause email messages to be sent:

- When SIM messages occur
- When the Site Manager is unable to make contact with Hitachi Vantara
- When the Site Manager is unable to make contact with one of the monitored subsystems
- When GSC requests a system update



- When GSC requests a dump file to be generated and transmitted to Hitachi Vantara

Whether or not the Site Manager sends an email for each of these events is individually configurable. In other words, you can configure the Site Manager to send email messages only when SIMs occur, only when the Site Manager cannot contact Hitachi Remote Ops, both, or neither.

Configuring Notifications

For the Site Manager to send email messages, it is necessary to know the IP address or host name of the customer's email server, and whether or not authentication is required by that server. If authentication is required by the customer's email server, you will need to obtain an SMTP user account and password from the customer for use with their email server.

The **AutoDumps** option enables the Site Manager to send an email when it receives a request to generate a dump. This request can come from Hitachi Remote Ops, from the Site Manager generating a dump in response to a SIM, from the Service Manager, or from the Web Interface.

The **Center transport failure** option enables the Site Manager to send an email when it is unable to contact the Hitachi Remote Ops. The Site Manager will not send an email for every failure to contact the Center. It will send one email message after it has exhausted all of the retries of each configured contact method and exhausted the number of sequence passes configured on the Center tab. See [Configuring the Center Tab](#) for more detail about these settings.

This is a fairly rare occurrence, and a condition about which a CSR and a customer should want to be notified.

The **Microcode updates** option enables the Site Manager to send an email when it receives a request to perform a system update, and when the upgrade completes or returns an error. This request can only come from Hitachi Remote Ops.

The **SIMs** option enables the Site Manager to send email messages for SIMs. SIM messages are not summarized. Use the **SIM Severity** control to restrict notifications based on the level of the SIM. For example, you can select Acute and Serious from the list to limit email reporting to SIMs with these levels. The default value of the combo box is "All" indicating that Site Manager should send an email for each SIM that occurs.

A valid, non-manual contact method must also be defined in order for SIM notification to occur. Having no contact methods configured or a manual contact method configured will preempt SIM processing and bypass any SIM email notification.

The **Subsystem connection failure** option enables the Site Manager to send an email when it is unable to contact a subsystem for more than one hour. The Site Manager will not send an email for every failure to contact the subsystem.

Mail server: Enter the host name or IP address of the customer's mail server. The customer will have to provide this information.

Port: Enter the SMTP port number. The standard SMTP port is 25.

From: A "From" identity is required. If the customer's email server requires authentication, you will need to put the new



email address obtained from the customer in this control, e.g. HitachiVantara_Support@customername.com. If the customer's email server does not require authentication, you can often supply a fictitious (but more descriptive) identity, e.g. HitachiVantara-VSP5000-30032@customerCompany.com. Either way, what you supply in the From address needs to look like a valid email address and include the @ sign and no space characters. Also, be aware that a fictitious email address may result in email messages from the agent to be marked as spam by filters. However with most filters you can usually mark them as "not spam".

Use authentication, SMTP user, and password: When you get permission or a request from the customer to send email messages, you will need to collect some information from them about their mail server: its host name or IP address and whether or not it requires authentication from inside of their firewall are the first two questions to ask. It is common for organizations not to require authentication to send an email from inside of their firewall. If their server does require authentication, the next question to ask is if they will provide you with an email account for the Site Manager to use. If they provide you with an email address to use, use that address in the From box, check the **Use authentication** checkbox, and enter the SMTP username and password in the text boxes provided.

Use SSL: Specifies whether SSL is used to access the specified SMTP mail server. The mail server is required to support secure connections and advertises STARTTLS in the response to the EHLO command.

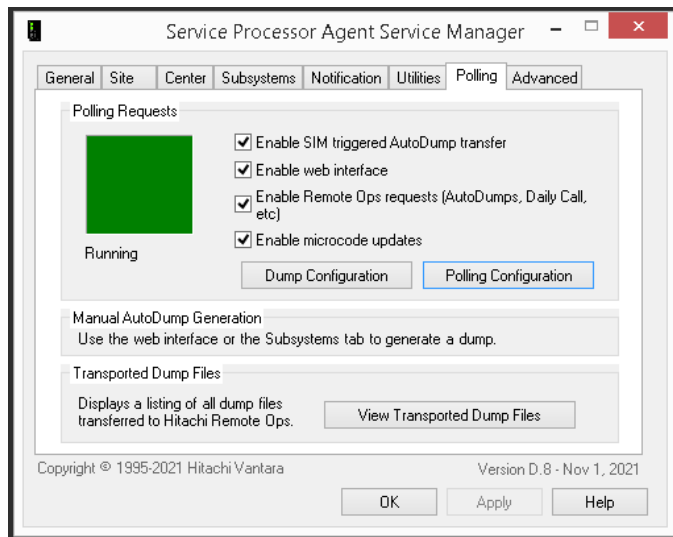
Email addresses: Enter each email address you want the Site Manager to send messages to in this text box. Separate the list of addresses by putting each one on a separate line.

Send email as plain text only: Choose this option to send emails in a plain text format instead of using a rich text/HTML format.

Send Test Email: Be sure to test your email settings and addresses before leaving the site. To test your settings, click **Send Test Email**. The Site Manager will send a test message immediately or describe any problems it encounters with your email settings.



Configuring the Polling Tab



On the **Polling** tab, the best practice recommendation is to enable everything within the **Polling Requests** panel.

The **Enable SIM triggered AutoDump transfer** option determines whether or not a SIM can trigger the generation and transfer of a Detail dump to Hitachi Remote Ops. The dump will only be triggered for SIMs with particular reference codes.

The **Enable web interface** option starts and stops the **Web Interface**. This feature enables users who don't have access to a Site Manager's SVP but who do have access intranet or internet access to the SVP to use the Web Interface to request dumps.

The **Enable Remote Ops requests** option starts and stops polling of Hitachi Remote Ops for various requests: dumps, system updates, SVP reboots, daily call, software updates for the Service Processor Agent. The polling settings can be changed by clicking the **Edit Polling Configuration** button. More on these settings can be found in the [Remote Ops Polling](#) section.



Finalizing the Configuration

Return to the **General** tab and click **Apply**. The **Apply** button and the **OK** button will perform checks on your configuration. You may receive one or more error messages or warnings if your configuration is incomplete. If this occurs, correct any errors before attempting to **Apply** again.

If you apply changes and the services are stopped, the Service Manager will ask if you want to start the services. Clicking **Yes** will start the services and should cause the red visual cues to turn green.

You can open logs from the **General** tab if you would like to watch the startup process.

Finalizing the SVP Agent

Follow the guidelines in the [Testing](#) section to test connectivity between the Site Manager and the SVP Agent

Finalizing the Site Manager

Follow the guidelines in the [Testing](#) section to test connectivity between the Site Manager and each SVP Agent, as well as the connection between the site and Hitachi Remote Ops.

After Testing

We recommend closing log windows when you are finished viewing them. Leaving them open permanently will unnecessarily add to network traffic and overhead and consume memory resources on the SVP.

Click **OK** to minimize the Service Manager to the system tray.



Service Processor Agent Operations

Testing

Once you have installed, configured, and started the application, you can use the Service Manager on the Site Manager to test network connectivity to the systems being monitored and to test that all systems are able to generate configuration data.

Testing Daily Call

To test collection of configuration data:

- Open the Site Manger logs
- Click on the **Utilities** tab
- Check **Generate new data files**
- Click **Transfer Now**
- View the progress in the log

Testing Collection of Configuration Data for a System

To test collection of configuration data for a particular system:

- Click on the **Subsystem** tab
- Double-click on the desired system
- Click **View Log** to open the SVP Agent log
- Click the **Generate Data Files** button
- View the progress in the log

Testing Dump Collection

The site manager must also be running to test dump collection, because the generated dump is transferred to Hitachi Remote Ops (or wherever the transport method points).

To test:

- Click on the **Subsystem** tab.
- Double-click on the desired system
- Click **View Log** to open the SVP Agent log
- Click the **Generate Dump File** button
- Select the desired dump type from the pop-up window and click **Generate**



- View the progress in the log

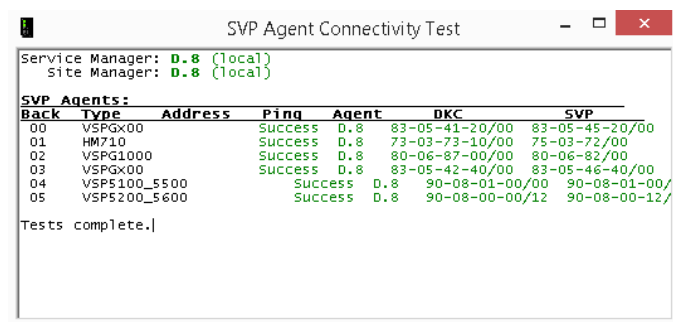
A system will enter a 2 hour lockout period after each successful dump generation, during which any subsequent requests will be refused until the lockout period expires.

Testing Network Connectivity with the Site Manager

To test network connectivity:

- Ensure that the Site Manager service is running
- Ensure that the SVP Agent service is running on all systems
- Select the **Utilities** tab
- Click the **Test Now** button
- View the SVP Agent Connectivity Test report
 - If the report is displaying application version information for a system, then the SVP Agent is functioning normally on that system

At a properly configured site, the report should look like this:



SVP Agent Connectivity Test

Service Manager: D.8 (local)
Site Manager: D.8 (local)

SVP Agents:

Back	Type	Address	Ping	Agent	DKC	SVP
00	VSPGX00		Success	D.8	83-05-41-20/00	83-05-45-20/00
01	HM710		Success	D.8	73-03-73-10/00	75-03-72/00
02	VSPG1000		Success	D.8	80-06-87-00/00	80-06-82/00
03	VSPGX00		Success	D.8	83-05-42-40/00	83-05-46-40/00
04	VSP5100_5500		Success	D.8	90-08-01-00/00	90-08-01-00/
05	VSP5200_5600		Success	D.8	90-08-00-00/12	90-08-00-12/

Tests complete.

Testing Network Connectivity with the SVP Agent

On the SVP Agent, to test network connectivity to the Site Manager:

- Open the Service Manager
- Ensure that the SVP Agent service is running
- Ensure that the Site Manager service is running
- Select the **Utilities** tab
- Click the **Test Now** button
- View the SVP Agent Connectivity Test report

At a properly configured site, the report should look like this:



```
SVP Agent Connectivity Test
Service Manager version: 0.8
SVP Agent version: 0.8
Site Manager version: 0.8
Tests completed successfully.
```

The line labeled **Site Manager** indicates whether the back is able to communicate with the the front. If you see any error messages, it indicates that either the Site Manager service is not running on the Site Manager or that there is no TCP/IP connectivity to the Site Manager on the required ports.



Dump Generation

There are four methods of generating and transferring dumps to Hitachi Remote Ops:

- SIM Triggered Dumps
- Through the Service Manager
- Through the Web Interface
- From Remote Ops Polling

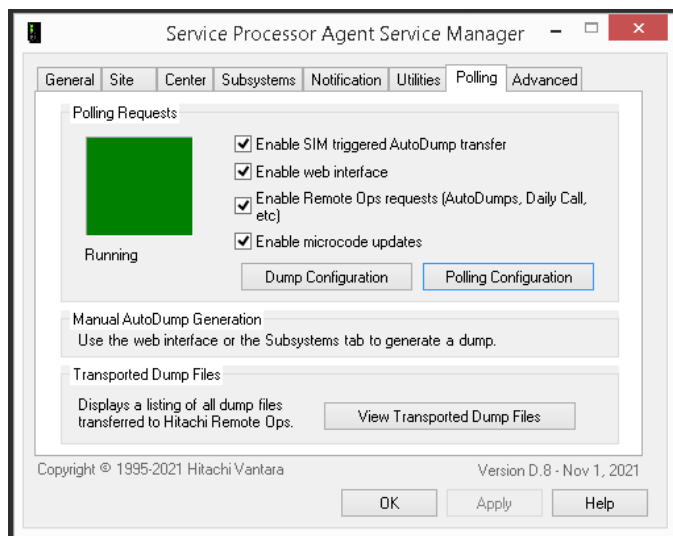
Whichever method is used, the system will enter a 2 hour lockout period after each successful dump generation, during which any subsequent requests will be refused until the lockout period expires.

Transferring dumps to Hitachi Remote Ops requires contact information to be configured on the Site Manager. Follow the directions in the [Configuring the Center Tab](#) to populate and learn how to use the controls on the **Center** tab.

Note: Attempts to transfer a dump will time out after 8 hours.

SIM Triggered Dumps

Under the **Polling** tab, the **Enable SIM triggered AutoDump transfer** option determines whether or not a SIM can trigger the generation and transfer of a Detail dump to Hitachi Remote Ops. SIM triggered dumps will only be triggered for SIMs with particular reference codes.



Service Manager

From the Service Manager, you can trigger a dump by:

- Selecting a system from the **Subsystems** tab
- Clicking **Properties**



- Clicking **Generate Dump File**
- Selecting an dump type
- Clicking **Generate**

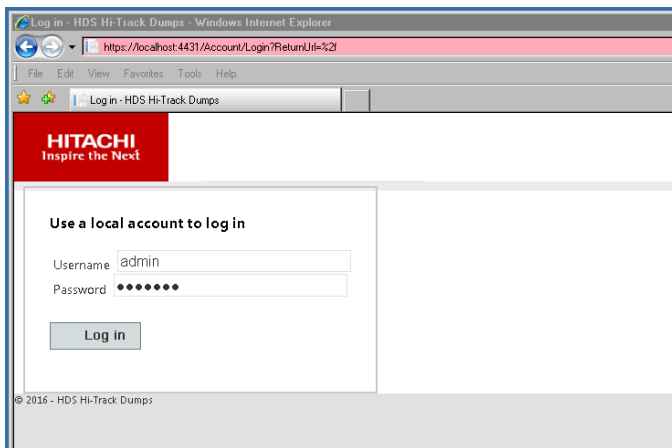
You can view the progress of the dump from the SVP Agent log and the progress of the transfer from the Site Manager log.

Web Interface

There are two ways to access the Web Interface:

- The Web Interface shortcut in the Start menu
- The address **https://IP:PORT/** where **IP** is the front's IP address and **PORT** (the default value is 4431) is the port that was configured during installation. IP can also be replaced with "localhost" as the url when on the Site Manager itself.

Either will navigate you to the web application. By default, you will be notified by the browser that the default self-signed SSL certificate provided by the application is not trusted and prompted by your browser about whether or not you'd like to proceed to the Web Interface. After proceeding, you'll pull up the login to the Web Interface.

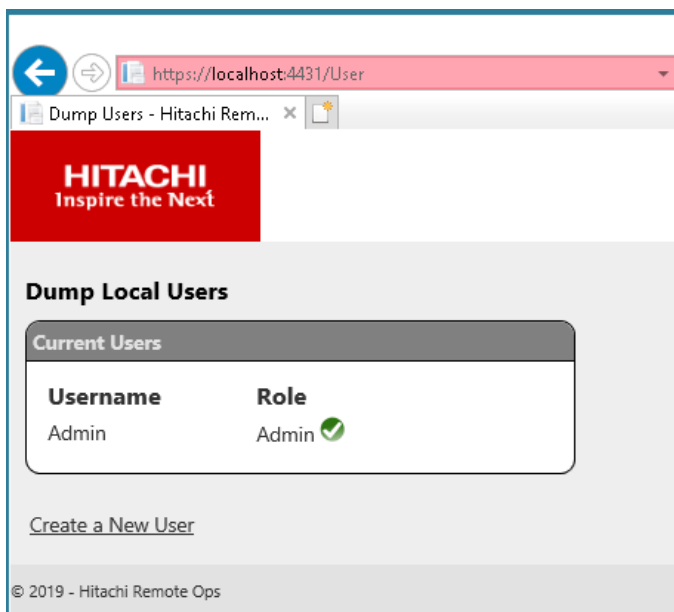


The initial administrative login user is "admin" and the password is "default". Upon logging in, the administrator will be prompted to change their password.

We recommend configuring a secure local administrator or configuring LDAP authentication upon logging in the first time.

User Administration

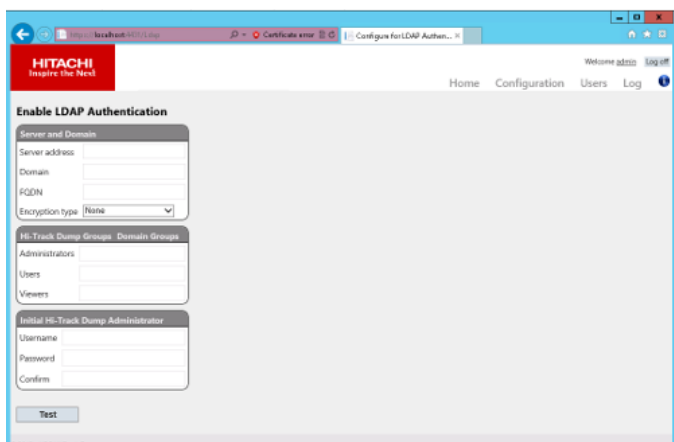




Additional users may be added by clicking the **User** navigation link at the top and then the **Create a New User** link. Web Interface users can be assigned one of the following role:

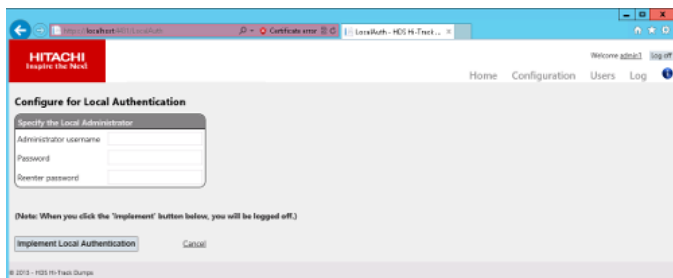
- **Viewer:** This group can only view a Site Manager's systems and the logs.
- **User:** This group can only view a Site Manager's systems, submit dump requests, and view the logs.
- **Admins:** This group can do everything a User can do and can also edit the Web Interface's configuration, enable or disable dump and microcode update (aka system update) polling, edit users, and view the logs.

LDAP authentication can be configured by navigating to **Configuration**, clicking **Edit**, and filling out the fields on that page. Once completed, click **Test** to verify the LDAP configuration. Once verified, an **Implement Now** button will appear. Re-enter the "Initial Administrator" password and then press **Implement Now** to commit the changes.



Local authentication may be re-enabled by editing the **Configuration** and clicking **Implement Local Authentication**. You will be prompted to set up a new Local Administrator username and password. Then you will have to click **Implement Local Authentication** again to commit the changes.





The list of available systems to select can be found on the **Home** page, or a warning message if the **Site Manager** isn't currently running. Select the desired systems by checking the boxes next to their serial number. Click **Submit Dump** when finished with your selection.

On the next screen, enter the numerical portion of an case number if you want to associate the dump request with a case. Then select the desired dump type from those available. If batching a request for multiple systems, the dump types available will be limited to those of the system type with the most dump type restrictions.

Once submitted, you'll be prompted to return either to **Home** or view the progress of the dump request in the **Log**.

In the **Log**, you can sort messages by the date range or severity. You can also choose to have the log permanently scrolled to the bottom to view the latest messages as they come in. Also, you can delete a range of messages by clicking **Clear** and selecting a date range, or save the logged messages to a CSV file by clicking **Export**.

Installing a Customer Certificate

If a customer would like to install their own SSL certificate for the Web Interface, they may do so manually with the following procedure. The customer will need the thumbprint (with white spaces removed) of the certificate to be installed on hand, as well as the port that the Web Interface is bound to.

- Import the customer supplied SSL certificate into the Windows certificate store
 - Open the *Command Prompt* with administrative privileges
 - Enter *mmc* to open the Microsoft Management Console
 - Click *File*
 - Select *Add/Remove Snap-in*
 - Select *Certificates*
 - Select *Computer account* and click *Next*
 - Select *Local computer* and click *Finish*
 - Click *OK*
 - Expand *Certificates (Local Computer)*
 - Expand the certificate store that you will be installing the SSL certificate into
 - Right click *Certificates*
 - Expand *All Tasks* and select *Import*
 - Follow the prompt to select the customer supplied SSL certificate and input into the certificate store
 - Repeat step **l** through step **m** to import the certificate's private key if the private key was not packaged together



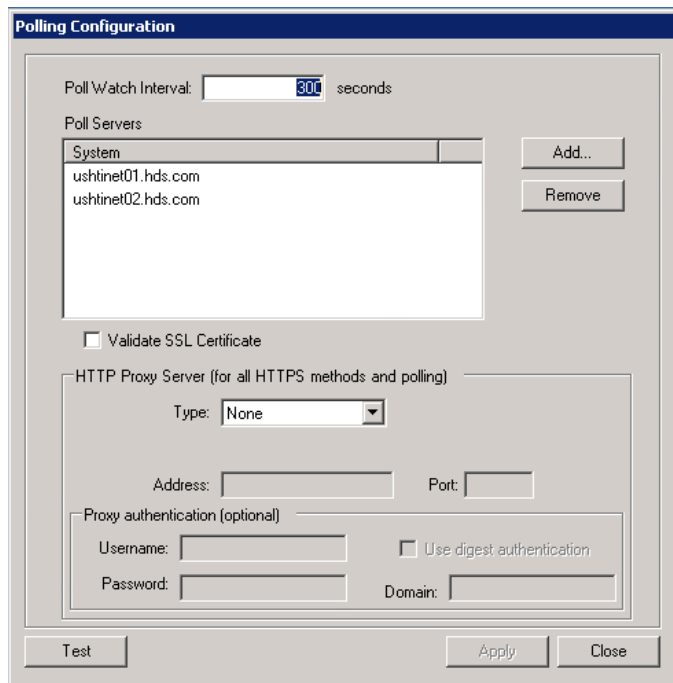
with the certificate in a standard encrypted file

- If the imported certificate from this step does not display a key symbol in the top left corner of the certificates icon, that means only a certificate has been imported and that you need to import the certificate's private key as well.
- From a command prompt, run `netsh http delete sslcert ipport=0.0.0.0:4431`
 - Replace `4431` with the port configured at installation if the default configuration was not used
- From a command prompt, run `netsh http add sslcert ipport=0.0.0.0:4431 certhash=thumbprint appid={GUID}`
 - Replace `4431` with the port configured at installation if the default configuration was not used.
 - Replace `thumbprint` with the thumbprint of the customer supplied SSL certificate
 - Replace `GUID`, but not the braces surrounding it, with the GUID of the Hitachi Remote Ops Service Processor Agent version installed. See [Technical Information](#) for the list of GUIDs for each version of the application.

Remote Ops Polling

From the Site Manager, you can enable the application to poll Hitachi Remote Ops for remote support functions like dump requests or system updates. This setting is enabled by default and can be controlled from the **Polling** tab with the **Enable Remote Ops requests**. If enabled, the Site Manager will complete requests for dumps and system updates that come in from Hitachi Remote Ops.

If there is a need to edit or test the settings that the Service Processor Agent uses to poll Hitachi Remote Ops for system updates, that can also be done from the **Polling** tab by clicking **Edit Polling Configuration**. The Site Manager will poll at intervals correlating to the configured number of **Poll Watch Interval** seconds and cycle through the servers listed under **Poll Servers** with every subsequent poll for requests. Connectivity to the poll servers can be tested by clicking **Test**. If the site requires a proxy and/or authentication in order to reach the poll servers from the customer network, these settings can be configured here as well.



The image shows a 'Polling Configuration' dialog box. At the top, 'Poll Watch Interval' is set to 300 seconds. Below this is a 'Poll Servers' list containing 'ushtinet01.hds.com' and 'ushtinet02.hds.com', with 'Add...' and 'Remove' buttons. A checkbox for 'Validate SSL Certificate' is unchecked. The 'HTTP Proxy Server (for all HTTPS methods and polling)' section has a 'Type' dropdown set to 'None', and fields for 'Address' and 'Port'. Below that, 'Proxy authentication (optional)' includes fields for 'Username', 'Password', and 'Domain', along with a checkbox for 'Use digest authentication'. At the bottom are 'Test', 'Apply', and 'Close' buttons.



System Updates

You can enable remote system updates by following the instructions above to enable Remote Ops Polling.

It is not possible to trigger a system update directly from the Site Manager through the Service Processor Agent for security reasons.



Monitoring the Service Processor Agent

When the Service Processor Agent starts up for the first time, it creates a **C:\HDS** directory for output generated by application. Detailed log files are generated and placed in the **C:\HDS\Logs** directory. There are variety of log files types.

- Site Manager logs
 - These have a "-Front" suffix
- SVP Agent logs
 - These have a "-Back" suffix
- Service Monitor logs
 - These have a "-SvcMon" suffix
- Service Manager logs
 - These have a "-SvcMgr" suffix
- Transport logs
 - These are within "Transport.log"

For the first three types of logs, new log files are created each day so long as the relevant service is running. The log's date will be a part of the file name. For example, the file name for a Site Manager log from February 14, 2018 would be "20180214-Front.log". Service Manager are similar but will only exist on days for which the Service Manager has been actively used.

For these four types of logs, any logs older than 30 days are deleted every day.

The transport log contains a record of every transfer attempted from this Site Manager and whether the transfer succeeded or failed. This log is never deleted or overwritten.

Viewing Log Files in the Service Manager Application

From the Service Manager, you can view the current day's local log files by clicking the appropriate button on the **General** tab. The logs available will depend on how the Service Processor Agent is configured and whether it is running on a storage product. The transport log cannot be viewed through the Service Manager.

The Service Manager can only be used to display the log file for the current day. To view previous log files files, select the log you would like to view from **C:\HDS\Logs** and double-click it to open it in Notepad.

Viewing Log Files Remotely

From the Site Manager, you can also view the SVP Agent logs of remote SVP Agents. To do this:

- Go to the **Subsystems** tab
- Double-click the system in which you are interested
- Click **View Log**



Remote logs will similarly only display the log file for the current day. To view previous log files on a remote SVP Agent, you need to establish a Remote Desktop connection into the remote SVP, and select the desired log from **C:\HDS\Logs**.

Sending SVP dumps to Hitachi Remote Ops

From the Site Manager, you can send a manually generated SVP dump to Hitachi Remote Ops. To do this:

- Go to the **Subsystems** tab
- Double-click the system in which you are interested
- Click **Transport Dump Files**
- Select the dump file you want to send and click **Send**

Sending a dump file to the Center this way does not create a new dump file. It only allows you to choose an existing dump file on the particular system. If you need to send a current dump file, you must either remote desktop to the SVP and generate the dump file first or use one of the dump generation methods listed in [Dump Generation](#).

Note: Transferring a dump will time out after 8 hours.

Testing a Contact Method

On the **Utilities** tab of the Service Manager on the Site Manager, you can perform a test call to Hitachi Remote Ops by clicking the **Transfer Now** button.

If you want to test a particular contact method:

- Click the **Center** tab
- Double-click a contact method
- Click **Test**



Email Notification Templates

Templates for various email notifications sent by the Service Processor Agent have been provided in the following subsections. Please note that the subsection header, e.g. "SIM Alerts", is not part of the template for the email notification.

Bracketed numbers, e.g. {0}, are placeholders for information relevant to the alert.



SIM Alerts

```
<html>
<head>
</head>
<body>
<p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">This is an automated message
generated by the Hitachi Vantara storage system referenced below. Do not reply
to this message.</span></font></p>
<table border="1" style="border-collapse: collapse" id="table1">
  <tr>
    <td><font face="Verdana" size="2">Site ID:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{0}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Site name:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{1}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System type:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{2}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System serial number:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{3}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Log number and index: </font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{4}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Date and time:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{5}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Reference code:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{6}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Error section:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{7}</font></td>
```



```

</tr>
<tr>
  <td><font face="Verdana" size="2">Error detail:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{8}</font></td>
</tr>
<tr>
  <td><font face="Verdana" size="2">Error location:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{9}</font></td>
</tr>
<tr>
  <td><font face="Verdana" size="2">Alert level:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{10}</font></td>
</tr>
<tr>
  <td><font face="Verdana" size="2">Status:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{11}</font></td>
</tr>
</table>
<br/>
<font face="Arial" size="1">
  <span style="font-size: 8pt; font-family: Arial">This email is provided as a supplement and is not a replacement for
Hitachi Remote Ops
  reporting to the Hitachi Vantara Support Center call management system. The format of this message may change
at any time.
  </span>
</font>
<hr/>
</body>
</html>

```



SIM HDD Alerts

```
<html>
<head>
</head>
<body>
<p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">This is an automated message
generated by the Hitachi Vantara storage system referenced below. Do not reply
to this message.</span></font></p>
<table border="1" style="border-collapse: collapse" id="table1">
  <tr>
    <td><font face="Verdana" size="2">Site ID:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{0}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Site name:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{1}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System type:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{2}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System serial number:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{3}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Log number and index: </font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{4}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Date and time:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{5}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Reference code:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{6}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Error section:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{7}</font></td>
```



```

</tr>
<tr>
  <td><font face="Verdana" size="2">Error detail:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{8}</font></td>
</tr>
<tr>
  <td><font face="Verdana" size="2">Error location:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{9}</font></td>
</tr>
<tr>
  <td><font face="Verdana" size="2">Alert level:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{10}</font></td>
</tr>
<tr>
  <td><font face="Verdana" size="2">Status:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{11}</font></td>
</tr>
<tr>
  <td><font face="Verdana" size="2">HDD Serial number:</font></td>
  <td><font face="Verdana" size="2" color="#0000FF">{12}</font></td>
</tr>
</table>
<br/>
<font face="Arial" size="1">
  <span style="font-size: 8pt; font-family: Arial">This email is provided as a supplement and is not a replacement for
Hitachi Remote Ops
  reporting to the Hitachi Vantara Support Center call management system. The format of this message may change
at any time.
  </span>
</font>
<hr/>
</body>
</html>

```



Dump Requests

```
<html>
<head>
</head>
<body>
<p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">This is an automated message
generated by the Hitachi Vantara storage system referenced below. Do not reply
to this message.</span></font></p>
  <p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">An AutoDump has been requested. The details are
below:</span></font></p>
<table border="1" style="border-collapse: collapse" id="table1">
  <tr>
    <td><font face="Verdana" size="2">Site ID:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{0}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Site name:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{1}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System type:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{2}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System serial number:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{3}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Dump type: </font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{4}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Date and time:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{5}</font></td>
  </tr>
</table>
<br/>
<font face="Arial" size="1">
  <span style="font-size: 8pt; font-family: Arial">This email is provided as a supplement and is not a replacement for
```



Hitachi Remote Ops

reporting to the Hitachi Vantara Support Center call management system. The format of this message may change at any time.

<hr/>

</body>

</html>



System Update Requests

```
<html>
<head>
</head>
<body>
<p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">This is an automated message
generated by the Hitachi Vantara storage system referenced below. Do not reply
to this message.</span></font></p>
  <p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">A microcode update has been requested. The details are
below:</span></font></p>
<table border="1" style="border-collapse: collapse" id="table1">
  <tr>
    <td><font face="Verdana" size="2">Site ID:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{0}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Site name:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{1}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System type:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{2}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System serial number:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{3}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">DKC Version: </font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{4}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Start time (UTC):</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{5}</font></td>
  </tr>
</table>
<br/>
<font face="Arial" size="1">
  <span style="font-size: 8pt; font-family: Arial">This email is provided as a supplement and is not a replacement for
```



Hitachi Remote Ops

reporting to the Hitachi Vantara Support Center call management system. The format of this message may change at any time.

<hr/>

</body>

</html>



System Update Success Alert

```
<html>
<head>
</head>
<body>
<p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">This is an automated message
generated by the Hitachi Vantara storage system referenced below. Do not reply
to this message.</span></font></p>
  <p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">A microcode update has completed. The details are
below:</span></font></p>
<table border="1" style="border-collapse: collapse" id="table1">
  <tr>
    <td><font face="Verdana" size="2">Site ID:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{0}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Site name:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{1}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System type:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{2}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System serial number:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{3}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Version: </font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{4}</font></td>
  </tr>
</table>
<br/>
<font face="Arial" size="1">
  <span style="font-size: 8pt; font-family: Arial">This email is provided as a supplement and is not a replacement for
Hitachi Remote Ops
  reporting to the Hitachi Vantara Support Center call management system. The format of this message may change
at any time.
  </span>
```



<hr/>
</body>
</html>



System Update Failure Alert

```
<html>
<head>
</head>
<body>
<p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">This is an automated message
generated by the Hitachi Vantara storage system referenced below. Do not reply
to this message.</span></font></p>
  <p><font face="Verdana" size="2">
<span style="font-size: 10pt; font-family: Verdana">A microcode update has {0}. Hitachi Vantara Support Center will
review this. The details are below:</span></font></p>
<table border="1" style="border-collapse: collapse" id="table1">
  <tr>
    <td><font face="Verdana" size="2">Site ID:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{1}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">Site name:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{2}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System type:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{3}</font></td>
  </tr>
  <tr>
    <td><font face="Verdana" size="2">System serial number:</font></td>
    <td><font face="Verdana" size="2" color="#0000FF">{4}</font></td>
  </tr>
</table>
<br/>
  <font face="Arial" size="1">
    <span style="font-size: 8pt; font-family: Arial">This email is provided as a supplement and is not a replacement for
Hitachi Remote Ops
    reporting to the Hitachi Vantara Support Center call management system. The format of this message may change
at any time.
    </span>
  </font>
</hr>
</body>
</html>
```



Troubleshooting

Knowledge

For any issues with the Service Processor Agent not covered in this section, please reference Hitachi Vantara's Knowledge portal. Search Knowledge for information about the problem you are experiencing, and in the absence of a solution, ensure that you follow the escalation procedure for Hitachi Remote Ops issues, which can also be found on Knowledge.

System updates are failing and the SVP Agent says that it cannot fetch the microcode from the Site Manager

- Verify that the Site Manager you are investigating is configured as the Site Manager for the device. If the device is functioning as its own Site Manager or is pointing to a different remote Site Manager, resolve the misconfiguration at the customer site. The application does not support multiple Site Managers monitoring the same SVP Agents

One or more devices from the site are not showing up in Remote Ops

- Verify through the Site Manager logs that the Site Manager is both running and successfully completing transfer to Hitachi Remote Ops.
 - If the Site Manager is stopped, start the Site Manager. If the Site manager was stopped abnormally, use the most recent logs and the Windows Event Viewer to investigate the cause for the service stoppage
 - If transfer to Hitachi Remote Ops is not completing, investigate and resolve the issue
- Verify that the Site Manager you are investigating is configured as the Site Manager for the device. If the device is functioning as its own Site Manager or is pointing to a different remote Site Manager, resolve the configuration issue at the customer site. Please refer to [Configuring a Site Manager](#). The application does not support multiple Site Managers monitoring the same SVP Agents
- Verify through the SVP Agent logs that the SVP Agent is running and that fresh data is being generated during daily call
 - If the SVP Agent is stopped, start the SVP Agent. If the SVP Agent was stopped abnormally, use the most recent logs and the Windows Event Viewer to investigate the cause for the service stoppage
 - If you see a message about "*System.IO.IOException caught: Not enough storage is available to process this command.*", follow the recommendation in that section of this Troubleshooting guide
 - If you see a message that "*Time out occurred in generating the csv.zip...*", follow the recommendation in that section of this Troubleshooting guide
 - If you see a message that "*Did not generate file.dat, but also didn't produce a fail status*" for files being generated during daily call, follow the recommendation in that section of this Troubleshooting guide
 - If you see a message that "*Serial Number API unexpectedly returned: 0x0000*", follow the recommendation in that section of this Troubleshooting guide
- Verify that the CSV data on the device is fresh
 - Open **C:\HDS**
 - Unzip csv.zip



- If the the file modified dates are older than a day and there are no messages in the SVP Agent logs about csv.zip failing to generate, follow the escalation procedure for Remote Ops issues in Knowledge and include this detail in your escalation

I see a message in the SVP Agent logs that *System.IO.IOException caught: Not enough storage is available to process this command*.

Check the virtual memory setting on the SVP and ensure the option is enabled to **Automatically manage paging file size for all drives**. Reboot the SVP after making the change.

This setting can usually be found in the OS by:

- Opening up the **Control Panel**
- Opening the **System** control
- Navigating to the **Advanced** tab
- Clicking **Settings** within the **Performance** control
- Clicking the **Advanced** tab within the **Performance Options** window
- Clicking **Change** in the **Virtual Memory** control
- Selecting **Automatically manage paging file size for all drives**

I see a message that the SVP Agent *Time out occurred in generating the csv.zip...*

Upgrade the application to the latest version and then attempt a daily call. If these messages persist in the SVP Agent logs, follow the escalation procedure for Remote Ops issues outlined in Knowledge.

I see message in the SVP Agent logs that the *Serial Number API unexpectedly returned: 0x000*

If the SVP Agent logs are consistently and currently showing those messages, please investigate the health of the SVP. Verify that the SVP is in a normal state and that the SVP services are running normally.

If the SVP Agent is running on a VSP N800, VSP N600, VSP N400, VSP G800, VSP F800, VSP G600, VSP F600, VSP G400, VSP F400, VSP G200, or VSP F200 storage product, ensure that the SVP services are set to automatically start-up when the system starts up. If the SVP services are not configured to automatically start with the system, then the SVP Agent will not be able to collect configuration data or SIMs when a system reboots until the SVP services are manually started.

I see *Did not generatedat, but also didn't produce a fail status* messages in the back logs.

Daily call relies on certain amounts of the CPU being available in order to complete successfully, particularly for generating DCR.dat, DEV.dat, DKC.dat, Einfo.dat, and HDEV.dat generation. Very CPU intensive process like daily disk defragmentation or CPU intensive virus scans can interfere with the SVP Agent's ability to generate a complete set of configuration data. In those cases, you should offset either the daily runtime of the other process or the Site



Manager's configured daily call time.

I installed the Service Processor Agent on a system with open SIMs and the Service Processor Agent does not report them.

The application cannot report SIMs that occurred before it was installed. It does not poll the SVP to determine if there are open SIMs. Rather, it is notified directly by the SVP application when a SIM occurs. Therefore, SIMs that occurred before installation will not be reported unless the setting to resent uncompleted SIMs is enabled.

Problems connecting to Site Managers or SVP Agents running version D.7 or lower

Versions D.8 and higher of the application are not backwards compatible with versions D.7 and lower. When upgrading the application at a site, the best practice is to upgrade the application on both the Site Manager and on all the systems that it is monitoring to the latest version.

Problems with Dial-Up, FTP, or FTPS contact methods

Dial-up, FTP, and FTPS contact methods are no longer supported by the application. Contact methods of these types that have persisted from prior versions will no longer work. Please configure the default HTTPS contact methods if you want the application to transport data to Remote Ops. Otherwise, delete all existing contact methods and configure a *Manual* contact method in order to prevent transport to Remote Ops.

Problems with the Setup program (Service Processor Agent Setup.exe)

The setup program checks to see if required components are installed on the target system and installs them if not. Then, it installs the Service Processor Agent. No problems with the setup program are known or anticipated. However, in the event that the setup program does not operate as expected, you can perform the Service Processor Agent installation manually.

The application has a dependency on Microsoft .NET Framework 4.6., which itself has a dependency on an operating system component called the Windows Installer 3.1. This component is installed automatically by Windows XP Service Pack 2. If you need to install the Service Processor Agent on a system that has not been updated to Service Pack 2, the preferred path of action is to upgrade the SVP to SP2 and apply all additional required patches. However, if this is not possible, you may upgrade the Windows Installer by applying the patch located in the **Prerequisites** directory of the installation media.

After applying SP2 or manually applying the Windows Installer patch, you may install the Service Processor Agent by following this procedure:

- Open the installation media directory
- Navigate to the **Service Processor Agent** directory of the installation media
- If Microsoft .NET Framework 4.6 is not already installed
 - Run **dotNetFx46_full_x86_x64.exe**
- If Microsoft IIS 8.0 Express is not already installed



- Run **iisexpress_8_0_RTM_x64_en-US.msi** on a 64-bit OS
- Run **iisexpress_8_0_RTM_x86_en-US.msi** otherwise
- If Microsoft SQL Service Compact Edition is not already installed
 - Run **SSCERuntime_x64-ENU.msi** on a 64-bit OS
 - Run **SSCERuntime_x86-ENU.msi** otherwise
- Run **SPA.msi** by double-clicking it. Follow the prompts on the screen and then Close on the final panel. If this installer presents you with the choices "Repair Service Processor Agent" and "Remove Service Processor Agent", then the Service Processor Agent is already installed and you may chose to cancel or repair the installation
- Launch the Service Manager application manually from the **Start** menu by selecting **All Programs/Hitachi Vantara/Service Processor Agent/Service Manager**

Problems installing the prerequisite software

The installer will automatically attempt to install any missing prerequisite software during installation.

If the installer encounters any problems installing any of the prerequisites, navigate to the **\Service Processor Agent** subdirectory within the installation media and run the installer for the software that has failed to install properly.

For Microsoft .NET Framework:

- Run **dotNetFx46_full_x86_x64.exe**

For Microsoft IIS Express:

- Run **iisexpress_8_0_RTM_x64_en-US.msi** on a 64-bit OS
- Run **iisexpress_8_0_RTM_x86_en-US.msi** otherwise

For Microsoft SQL Service Compact Edition:

- Run **SSCERuntime_x64-ENU.msi** on a 64-bit OS
- Run **SSCERuntime_x86-ENU.msi** otherwise

After resolving the issue with the prerequisite software installation, rerun the application installation.

The Service Manager icon does not appear in the System Tray

If you have installed the Service Processor Agent and the Service Manager icon does not appear in the System Tray:

- Verify that the application was installed in the directory specified at the time of installation. The default directories are **C:\Program Files\Hitachi Vantara\Service Processor Agent** and **C:\Program Files (x86)\Hitachi Vantara\Service Processor Agent**. If the application is missing, repair install the application
- Look in the directory **C:\Documents and Settings\Administrator\Start Menu\Programs\Startup** or **C:\Users\Administrator\Start Menu\Programs\Startup** and ensure that a shortcut exists in this directory to the file **ServiceMgr.exe** in the installation directory. If a shortcut does not exist, create one. Alternatively, repair install the installation



- To start the Service Manager without rebooting, double-click the file **ServiceMgr.exe** in the installation directory, or from the Start Menu, choose **All Programs/Hitachi Vantara/Service Processor Agent/Service Manager**. The Service Manager icon should appear in the System Tray

The Service Manager application does not appear when you double-click the Service Manager icon in the System Tray

It could be behind the SVP application or another application. Minimize any open applications and you should find the Service Manager application.

The service or services don't start, but no error is displayed or logged in the log files.

Check the system event log (Administrative Tools/Event Viewer). An error may have occurred before the services or service manager could initialize logging.

After re-installing the Service Processor Agent, the Service Manager application does not appear.

Check the system tray for the Service Manager icon.

When I click a Log button in the Service Manager application, no log window appears.

The log window may already be open and may have been positioned on a larger desktop in a location outside of the visible area on your desktop. Try clicking the **Arrange** button to reposition it for your desktop.

Web Interface configurations disappear when upgrading from C.7 or lower

Due to an incompatibility with versions C.7 and lower, the configuration of the Web Interface will reset when upgrading the application.

Problems displaying the Web Interface in Internet Explorer 8

The Web Interface is supported on Microsoft Internet Explorer 9 or above, Google Chrome, and Mozilla Firefox. It also displays on Internet Explorer 8, but with a diminished GUI experience and possible loss of date-picker functions for the Log page.

Previous versions of the application remain installed after upgrade

Normally, it is not necessary to uninstall previous versions of the application to upgrade to the latest version and not expected that prior versions of the application will persist after an upgrade. The exception to this is if you need to perform a manual installation from **SPA.msi** instead of from the installation package, **Service Processor Agent Setup.exe**.

In this case, you will need to use the *Windows Control Panel* to remove all prior versions that remain.



Technical Information

Normally, the you will control the services through the Service Manager. However, the applications services can also be controlled manually through the Windows Services applet or through a command prompt. The short names of these services are as follows:

- HroSvpAgentSiteManager
- HroSvpAgent
- HroSvpAgentMonSvc
- HroSvpAgentWebHost

Data Communication Ports

The Service Processor Agent uses four TCP ports for communicate between the Site Manager and SVP Agents. Ports 2056 and 2057 must be open for the services to work properly.

SVPs configured at the factory should always be pre-configured with these ports open. If the ports are not already open, they should not need to be opened manually. Each time the Service Manager starts up, it will attempt to whitelist the ports and services within the Windows firewall.

If a customer site is configured with storage subsystems on different subnets or VLANs with switches, routers, or NAT devices separating the subsystems, or if the customer firewall policies are very strict, the devices that the Service Processor Agent is installed on may be set to disallow TCP traffic between the subnets or VLANs destined for certain TCP ports. These devices may be set to allow traffic on a few well-known ports (21, 25, 80 and 8080 for example) and to disallow all other ports.

If it should prove to be impossible to use the default ports, these ports can be changed.

In the installation directory, which defaults to **C:\Program Files (x86)\Hitachi Vantara\Hitachi Remote Ops Service Processor Agent**, there is a file named **RemServer.config**. This is an XML file whose contents should look like the following:



If you change a port setting in this file and the Service Manager is running, it will notify you that the configuration file has changed and will ask if you would like to restart the services. Agree to restart the services and ensure that you make the same changes and restart the services on both the Site Manager and all SVP Agents.

GUIDs of Service Processor Agent Versions

The GUID for the Service Processor Agent is provided for the purpose of installing a customer supplied SSL certificate for use with the Web Interface, if desired, as detailed in the [Remote Operations](#) section. GUIDs are only provided for recent versions of the applications. If the version desired is not in this list, please upgrade to the latest release before attempting this operation.

- **D.8:** 6CDD4980-F46A-4AAC-8E3B-65B64FDD0CD1
- **D.7:** 34C076D2-EC6D-4965-A5C8-F8810A37FDDA

Email Templates

Templates for the emails sent by the application can be found in the [Email Templates](#) section.

