HITACHI
Inspire the Next

Hitachi Virtual Storage Platform Fx00 and Gx00

Service Processor Technical Reference

This guide is intended for system administrators, Hitachi Vantara representatives, and authorized service providers who install, configure, or operate VSP Gx00 models and VSP Fx00 models. In addition, this guide provides information about setup, configuring, and maintaining both physical and virtual service processor.

MK-97HM85045-01
October 2018

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara Corporation at https://support.hitachivantara.com/en_us/contact-us.html.

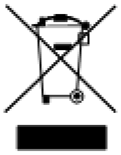
Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara Corporation.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Disposal



This symbol on the product or on its packaging means that your electrical and electronic equipment should be disposed at the end of life separately from your household wastes.

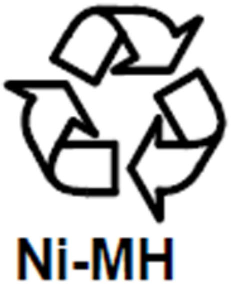
There are separate collection systems for recycling in the European Union. For more information, contact the local authority or the dealer where you purchased the product.

Recycling

A nickel-metal hydride battery is used in the Cache Backup Battery.

A nickel-metal hydride battery is a resource that can be recycled. When you want to replace the Cache Backup Battery, call the service personnel. They will dispose of it for you. This nickel-metal hydride battery, which is designated as recycling product by a recycling promotion low, must be recycled.

The mark posted on the Cache Backup Battery is a three-arrow mark that indicates a recyclable part.



Contents

Preface

Intended audience

This document is intended for Hitachi Vantara representatives, system administrators, authorized service providers, or customers who install, configure, and operate the VSP Fx00 models and VSP Gx00 models.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions
- RAID storage system hardware components and operational specifications

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. ▪ Indicates emphasized words in list items.
Italic	▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g` *`group`* (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`

Convention	Description
< > angle brackets	Indicates variables in the following scenarios: ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` ▪ Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

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

Icon	Label	Description
🗎	Note	Calls attention to important or additional information.
💡	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
⚠	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
⚠	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Changes in this revision

- Updated *Security patch and antivirus software* to reflect new policies related to Microsoft® Windows® and antivirus software upgrade path and installation.
- Revised table listing SVP OS and Hypervisor support for VSP Gx00 and Fx00 models.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1,000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1,000^3$ bytes
1 terabyte (TB)	1,000 GB or $1,000^4$ bytes
1 petabyte (PB)	1,000 TB or $1,000^5$ bytes
1 exabyte (EB)	1,000 PB or $1,000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

Product user documentation is available on Hitachi Vantara Support Connect: https://knowledge.hitachivantara.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

Hitachi Vantara Support Connect is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara Corporation.

Thank you!

Chapter 1: SVP overview

The Service Processor (SVP) provides out-of-band configuration and management of the storage system, and collects performance data for key components to enable diagnostic testing and analysis.

The Hitachi Vantara-provided SVP is available as a physical 1U management server or as a 64-bit software application. For this current version, the physical SVP server and SVP software applications are supported in the environments shown in the following table. For the latest interoperability updates and details, see the OS and Hypervisor Support for SVP: Service Processor for Virtual Storage Platform VSP Gxx0 and Fxx0 report.

		Minimum SVP version		
Operating System	Server/VM	VSP F400/F600/ F800 VSP G200/ G400/G600/ G800	VSP F350/F370/ F700/F900 VSP G350/G370/ G700/G900	Notes (additional requirements)
Windows 7 Professional	Bare metal install	83-01-03-x0/00	88-01-02-x0/00	
	VMware ESXi 6.0.0	83-03-02-x0/00	88-01-02-x0/00	
	KVM on Oracle Linux 7.2	83-03-23-x0/00	88-01-02-x0/00	3.8.13-98.7.1.el7uek.x86_64, qemu-kvm-1.5.3-105.el7.x86_64
Windows 7 Professional SP1	VMware ESXi 6.0 U2	83-03-23-x0/00	88-01-02-x0/00	Cluster is supported
Windows Server 2012	Bare metal install	83-01-03-x0/00	N/A	
	VMWare ESXi 6.0 U2	N/A	88-01-02-x0/00	
Windows Server 2012 R2	Bare metal install	83-01-03-x0/00	88-01-02-x0/00	
	Hyper-V Server 2012 R2	83-04-02-x0/00	N/A	
	VMWare ESXi 6.0 U2	N/A	88-01-02-x0/00	
Windows 8 Professional	Bare metal install	83-04-02-x0/00	88-01-02-x0/00	
Windows 10 Professional	Bare metal install	83-04-02-x0/00	88-01-02-x0/00	
Windows 10 Enterprise	Bare metal install	83-04-02-x0/00	88-01-02-x0/00	
	Hyper-V Server 2012 R2	83-04-02-x0/00	88-01-02-x0/00	

Operating System	Server/VM	Minimum SVP version		Notes (additional requirements)
		VSP F400/F600/ F800 VSP G200/ G400/G600/ G800	VSP F350/F370/ F700/F900 VSP G350/G370/ G700/G900	
Windows Server 2016	Bare metal install	83-04-27-x0/00	88-01-02-x0/00	
		83-04-47-x0/00		

The bare metal servers must meet the following requirements.

Item	Specification
Processor:	One core with hyper-threading, two cores without hyper-threading Processor performance comparable to Celeron 1.6 GHz
Random-access memory:	3.5 GB per storage system
Hard drive capacity:	120 GB per storage system
LAN connection:	One 1000Base-T

The following table lists SVP VM requirements.

VM platform	Requirements	Corresponding SVP guest OS
ESX Server	VMware ESXi server 6.0 Two quad core processors, Intel Xeon 2.29 GHz One port network interface card (NIC) 32 GB RAM	SVP guest OS (maximum one DKC per SVP guest OS) Two virtual CPUs One virtual network adapter 4 GB RAM 120 GB disk space
Linux KVM Server	Oracle Linux 7.2 Two quad core processors, Intel Xeon 2.29 GHz One-port NIC	Same as ESX Server

VM platform	Requirements	Corresponding SVP guest OS
	128 GB RAM	
Hyper-V Server	Hyper-V server 2012 R2 Two quad core processors, Intel Xeon 2.29 GHz One-port NIC 32 GB RAM	Same as ESX Server

Note: Only one storage array (DKC) can be managed per SVP software instance. Only one SVP software instance can be installed per OS instance. However, multiple virtual machines that each run their own OS/SVP software instance can be installed on a physical server. Other software is not supported when run in the same OS instance with the SVP software.

Chapter 2: Physical SVP (Windows 7 Enterprise) hardware description

The physical SVP with Windows 7 operating system is provided by Hitachi Vantara. The physical SVP is a 1U management server that attaches to each VSP disk controller (DKC). The following sections describe the front and rear panels of the Hitachi Vantara-supplied physical SVP, along with the physical, electrical, and environmental specifications.

SVP front panel

The front panel of the physical SVP is equipped with LEDs, a reset button, and a power button.

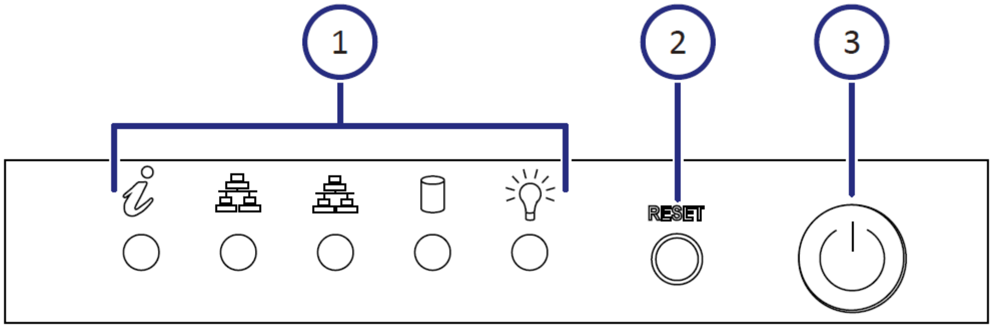


Table 1 SVP (Windows 7) front panel

Item	Description
1	LEDs. From left to right, the LEDs are: ▪ BMC Heartbeat ▪ LAN card 2 ▪ LAN card 1 ▪ Hard drive ▪ System standby power
2	Reset button.
3	Power button. Applies power to or removes power from the SVP.

SVP rear panel

The only ports used at the rear panel of the physical SVP are the power socket and the four LAN ports. The following ports connect to your IP network, the management console PC, and the user LAN port on each storage system controller.

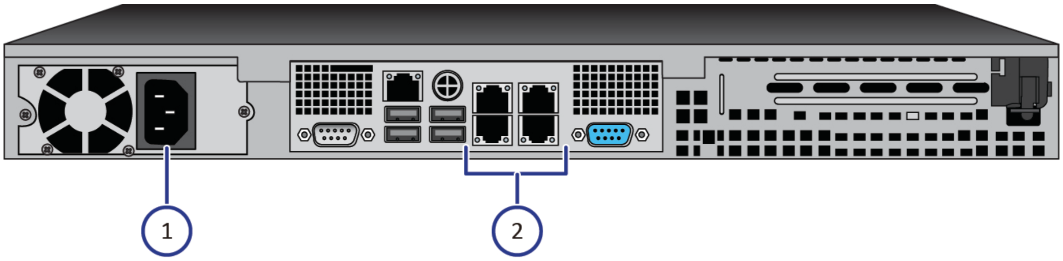


Table 2 SVP (Windows 7) rear panel

Item	Description
1	Power socket. Attach the power cable supplied with the SVP.
2	Four LAN ports arranged as follows: LAN3 LAN4 LAN1 LAN2 These ports connect to your IP network, the management console PC, and the user LAN port on each storage system controller.

Note: After the Initial Startup Wizard is run, the SVP can be used in non-bridge mode. In this mode, the cables can be removed from SVP ports LAN3 and LAN4 and attached to switches. For more information, contact customer support.

Service processor (Windows 7) hardware specifications

The following table lists the hardware specifications for the service processor (SVP) provided by Hitachi Vantara.

Caution: The SVP is not supported in high-temperature environments. Do not operate it in locations with temperatures above 40°C.

Item	Specification
Dimensions	Height: 1.7 inches (43 mm) Width: 17.2 inches (437 mm) Depth: 14.5 inches (369 mm) Weight: 14 lbs (6.4 kg)
Processor	Celeron G1820 2.7-GHz 2M, 2C, 2T ▪ Cores: 2 ▪ Instruction set: 64-bit ▪ SmartCache: 2 MB ▪ Maximum memory size: 32 GB ▪ Memory types: DDR3-1333, DDR3L-1333 @ 1.5V
Memory	8-GB RAM DDR3
Hard drive	2 TB
Network interface card	x4 ports (on-board NIC) + x1 IPMI (BMC) port
Fans	2 x 4-cm 4-pin PWM fans
Operating system	Windows Embedded Standard 7

Physical SVP (Windows 7) electrical specifications

The following table lists the electrical specifications for the physical SVP supplied by Hitachi Vantara.

Item	Specification
Rated AC voltage	100-240 V, 50-60 Hz, 4.2 - 1.8A
Power supply	350 W AC power supply with PFC
AC voltage	100-240 V, 50-60 Hz, 4.2 - 1.8 Amp
Power supply safety / EMC	▪ USA - UL listed, FCC ▪ Canada - CUL listed ▪ Germany - TUV Certified

Item	Specification
	▪ Europe/CE Mark ▪ EN 60950/IEC 60950-Compliant

MFT p-code	Description	watts
MBD-X10SLM+-LN4F-O	Single-socket H3 (LGA 1150) / 32-GB DDR3 ECC 1600 MHz / 6x SATA / 4x GbE	20 W
CSE-512F-350B	Two 350 W 3.5-inch internal drive bays	26.4 W
CM8064601483405	Intel Celeron G1820 2.7 Ghz 2M tray	53 W
0F11000	3.5-inch 25.4 mm 2 TB 32 MB 7200 RPM	9.1 W
KVR16E11S8	4 GB 1600 Mhz DIMM SR x8 with TS Kingston F	4.05 W
	Total	112.55 W

VA is 140.69, with a 0.8 power factor.

Note: The measurements are not kilo values.

Physical SVP (Windows 7) environmental specifications

The following table lists the environmental specifications for the physical SVP supplied by Hitachi Vantara.

Item	Specification
Operating temperature	41°F ~ 95°F (5°C ~ 35°C)
Non-operating temperature range	-40°F ~ 140°F

	(-40°C ~ 60°C)
Operating relative humidity range	8% ~ 90% (non-condensing)
Non-operating relative humidity range	5% - 95% (non-condensing)

Chapter 3: Physical SVP (Windows 10 Enterprise) hardware description

The physical SVP with Windows 10 Enterprise operating system is provided by Hitachi Vantara. The physical SVP is a 1U management server that attaches to each VSP disk controller (DKC). The following sections describe the front and rear panels of the Hitachi Vantara-supplied physical SVP, along with the physical, electrical, and environmental specifications.

SVP front panel

The front panel of the physical SVP with Windows 10 Enterprise operating system is equipped with LEDs, a reset button, and a power button.

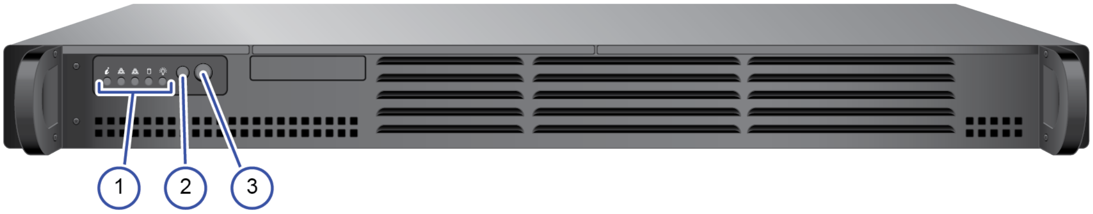


Table 3 SVP (Windows 10 Enterprise) front panel

Item	Description
1	LED (left to right): ▪ N/A ▪ LAN card 2 ▪ LAN card 1 ▪ Hard drive ▪ System standby power
2	Reset button
3	Power button

SVP rear panel

The only ports used at the rear panel of the physical SVP are the power socket and the four LAN ports. The following ports connect to your IP network, the management console PC, and the user LAN port on each storage system controller.

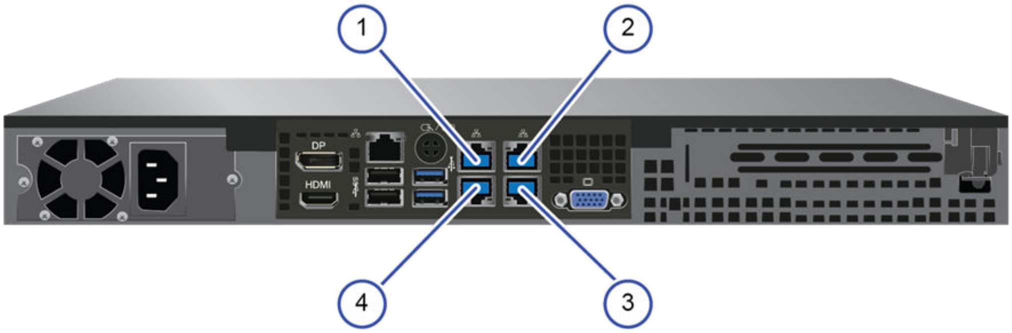


Table 4 SVP (Windows 10 Enterprise) rear panel

Item	Description
1	Management (DKC CTL1) - LAN3 port
2	Management (DKC CTL2) - LAN4 port
3	Maintenance - LAN2 port
4	Management (User) - LAN1 port

Note: The SVP running Windows 10 operating system does not provide an option to disable Spanning Tree Protocol (STP). If your network has BPDU enabled to prevent loops, connect the user LAN port on controllers 1 and 2 to an Ethernet switch that is also connected to the LAN1 port on the SVP.

Note: After the Initial Startup Wizard is complete, the SVP can be used in non-bridge mode. In this mode, the cables can be removed from SVP ports LAN3 and LAN4 and attached to switches. For more information, contact customer support.

Service Processor (Windows 10 Enterprise) hardware specifications

The following table lists the hardware specifications for the service processor (Windows 10 Enterprise) provided by Hitachi Vantara.

Item	Specification
Dimensions	Height: 1.7 inches (43 mm) Width: 17.2 inches (437 mm) Depth: 9.8 inches (249 mm) Weight: 10 lbs (4.5 kg)
Processor	Intel N3710 Pentium processor, 4C/4 threads, 1.6 GHz 2M cache, 6W
Memory	2 x 4 GB DDR3 1600MHz
Storage media	1 TB 5400 RPM SATA HDD
Network interface card	1-GbE x 4 ports (on-board NIC) x1 IPMI (BMC) port
Fans	2 x 4028 mm 13KPRM 4-pin PWM fans
Operating system	Windows 10 Enterprise
Maximum temperature	Up to 40° C (104° Fahrenheit) The SVP is supported in high-temperature environments. Do not operate in any location with temperatures above 40°C (104° Fahrenheit).

Physical SVP (Windows 10 Enterprise) electrical specifications

The following table lists the electrical specifications for the physical SVP provided by Hitachi Vantara.

Item	Specification
Rated AC voltage	100-240 V, 50-60 Hz, 4 - 2A
Power supply	200 W AC power supply
AC voltage	100-240 V, 50-60 Hz, 4 - 2 Amp
Power supply safety / EMC	▪ USA - UL listed, FCC ▪ Canada - CUL listed ▪ Germany - TUV Certified

Item	Specification
	▪ Europe/CE Mark ▪ EN 60950/IEC 60950-Compliant

Physical SVP (Windows 10 Enterprise) environmental specifications

The following table lists the environmental specifications for the physical SVP supplied by Hitachi Vantara.

Item	Specification
Operating temperature	41°F ~ 104°F (5°C ~ 40°C)
Non-operating temperature range	-40°F ~ 158°F (-40°C ~ 70°C)
Operating relative humidity range	8% ~ 90% (non-condensing)
Non-operating relative humidity range	5% - 95% (non-condensing)

Chapter 4: Installing the Hitachi Vantara-supplied SVP

Hitachi Vantara provides a 1U SVP for use with VSP Gx00 models and VSP Fx00 models. The SVP operates independently from the storage system's CPU and operating system.

The SVP provides out-of-band configuration and management of the storage system, and collects performance data for key components to enable diagnostic testing and analysis. The SVP runs the Windows Embedded Standard 7 or 10 Enterprise operating system, and is installed above the controller and drive trays in the rack.

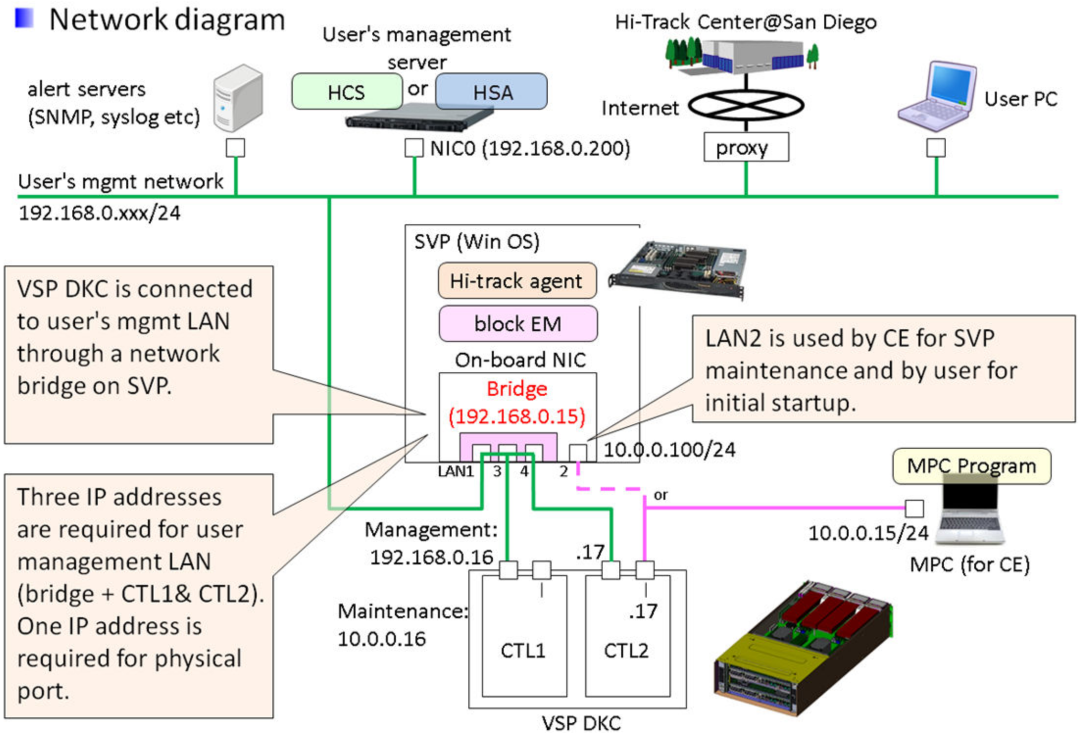
Important: The Hitachi Vantara-supplied SVP can only be installed, upgraded, or replaced by a Hitachi Vantara representative or an authorized service provider. Contact a Hitachi Vantara representative for more information about installing, upgrading, or replacing a Hitachi Vantara-supplied SVP.

Physical SVP network configuration

In networking terms, a *network bridge* is software or hardware that connects two or more networks so that they can communicate. For the physical SVP, a network bridge configures the three local-area network (LAN) ports on the SVP using the Bridge Connections setting in the Windows operating system. This configuration requires an external switching hub.

The following figure shows the physical SVP in a bridged network configuration.

Note: The Hitachi Vantara-supplied SVP running the Windows operating system cannot be used with the storage system if the SVP belongs to different subnets, and if a router or a firewall is filtering packets according to a defined condition. There is not a limit for distance between the server running the SVP application and the storage system being managed if they belong to the same subnet.

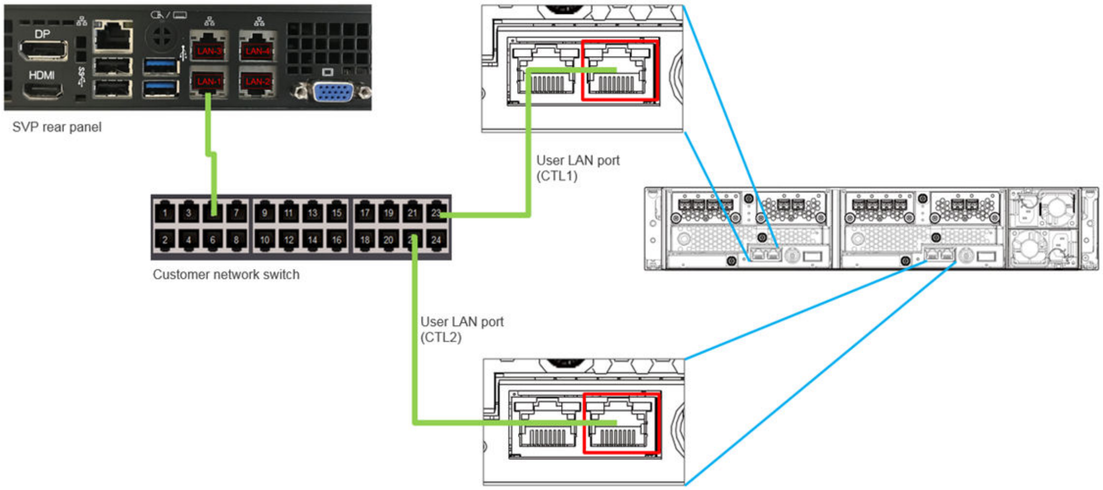


VSP DKC is connected to user's mgmt LAN through a network bridge on SVP.

LAN2 is used by CE for SVP maintenance and by user for initial startup.

Three IP addresses are required for user management LAN (bridge + CTL1& CTL2). One IP address is required for physical port.

The following figure shows a physical SVP in non-bridged environment.

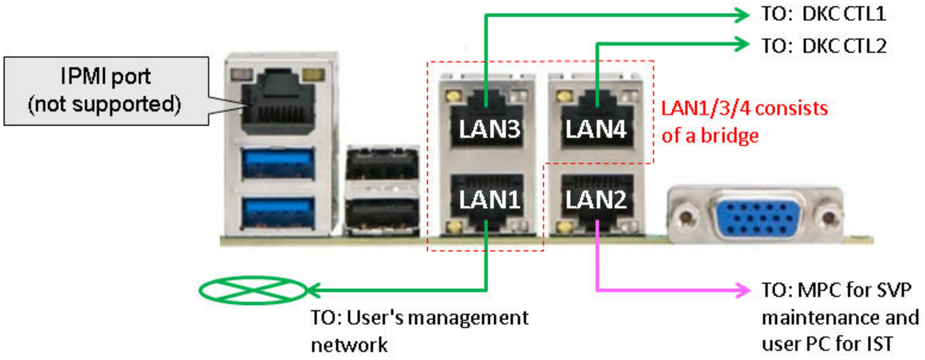


For information about configuring an SVP for a non-bridged network environment, see Operating the physical SVP in a non-bridged network configuration (on page 35) .

Physical SVP LAN port assignment

The LAN port assignments on the physical SVP should match the ones in the following figure.

The IPMI port is an IPMI-dedicated port connected to the BMC in the SVP and does not appear in the Windows operating system. For security reasons, the IPMI port cannot be enabled in the SVP BIOS setting and is not supported for the SVP.


TO: DKC CTL1
TO: DKC CTL2
IPMI port
(not supported)
LAN3
LAN4
LAN1
LAN2
LAN1/3/4 consists of a bridge
TO: User's management network
TO: MPC for SVP maintenance and user PC for IST

Default IP address settings

The physical SVP is pre-configured with a default IP addresses and bridge the LAN 1/3/4.

The user connects to the SVP using the IP address 192.168.0.15 for LAN1/3/4 ports (management) or 10.0.0.100 for LAN2 port (maintenance).

Port	Name of NIC (user can change a NIC name)	Connected to	Default IP address	IP address after bridge is configured	Notes
LAN 1	Management (User)	Management LAN	N/A (DHCP)	192.168.0.15 /24	Part of bridge. IST uses LAN1/3/4 or 2 ports for Remote Desktop Protocol (RDP).
LAN 2	Maintenance	MPC or User PC	10.0.0.100/24	-	Not a part of bridge. IST uses LAN1/3/4 or 2 ports for RDP.
LAN 3	Management (CTL1)	DKC CTL1	N/A (DHCP)	192.168.0.15 /24	Part of the bridge.
LAN 4	Management (CTL2)	DKC CTL2	N/A (DHCP)	192.168.0.15 /24	Part of the bridge.
IPMI	N/A	User PC	N/A (disabled)	-	Not supported (user's discretion)

Installing a physical SVP

The following describes how to install the physical SVP into a rack and configure it for your network environment.

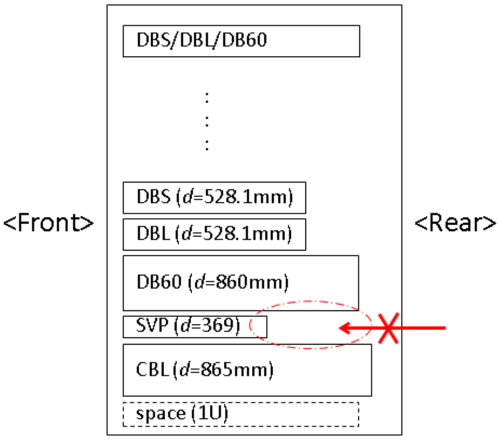
Caution: The physical SVP (Windows 7) is not supported in a high-temperature environment. Do not operate the SVP at temperatures above 95°F (35°C).

Caution: The SVP (Windows 10) is supported in a high-temperature environment. Do not operate the SVP at temperatures above 104°F (40°C).

Mounting the physical SVP

The physical SVP has a depth of 14.5 inches (369 mm). The 4U CBL controller and dense intermix drive tray (DB60) have a depth of 34.1 inches (865 mm) and 33.9 inches (860 mm), respectively.

If the SVP is rack-mounted between a CBL and DB60, as shown in the following figure, there is not enough space to access the rear I/O panel of the SVP.

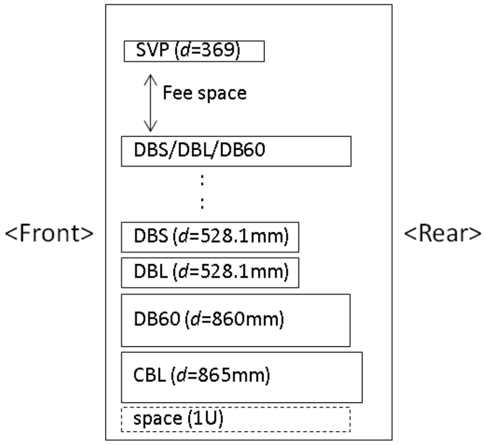


a) Bad example of rack-mounting with SVP

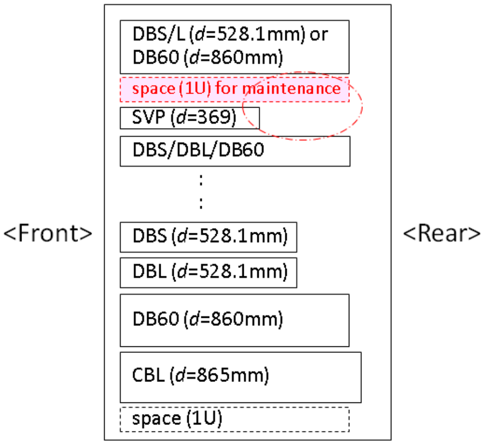
Rear I/O panel layout of SVP

To verify the SVP can be accessed for maintenance:

- Locate the SVP at the top of the rack or above the system.
- If a small form factor drive tray (DBS) or DB60 is added at the top of the rack, prepare a 1U space between the system and the small form-factor, large form-factor, and DB60 trays.



b1) Good example of rack-mounting with SVP



b2) Good example of rack-mounting with SVP

Choosing a mounting location

Mounting the physical SVP appropriately in the rack is critical to ensure optimum performance.

Procedure

1. Install the physical SVP in the top bay of the rack or as close to the top bay as possible.
2. Leave approximately 25 inches in front of the rack to enable you to open the front bezel.
3. Leave approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and ease in servicing.

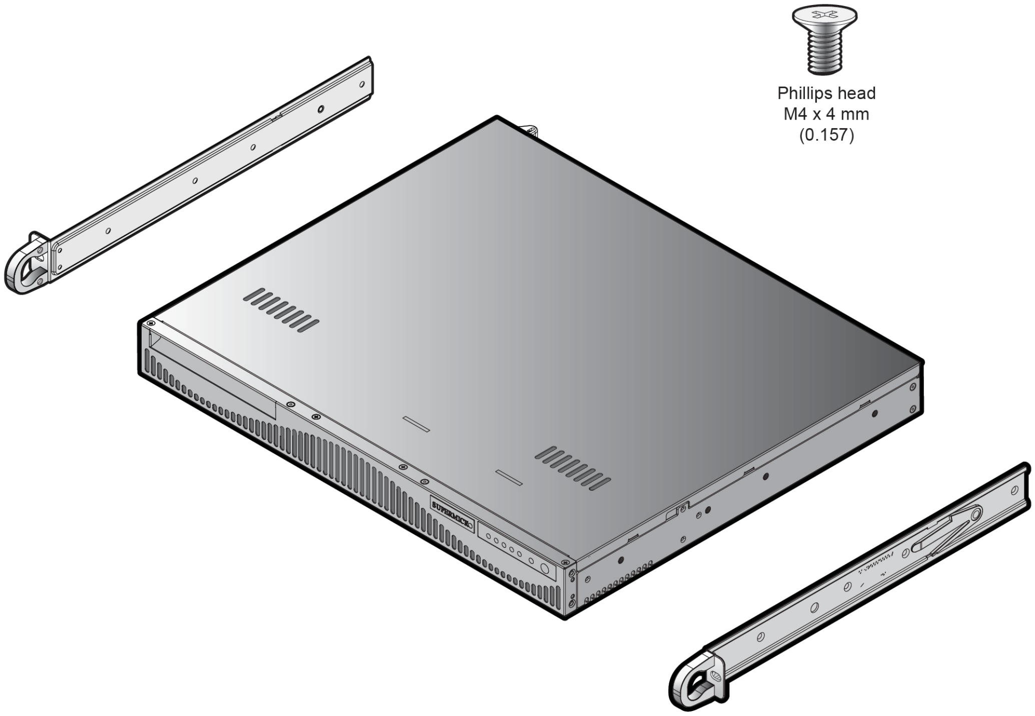
Installing the inner rail extension

The physical SVP contains two rack rail assemblies. Each assembly consists of an inner fixed chassis rail that secures directly to the SVP chassis, and an outer fixed-rack rail that secures directly to the rack itself.

The physical SVP includes chassis ears that you must remove before installing the rails.

Procedure

1. Remove the chassis ears.
   a. Locate and remove the three screws holding the chassis ear in place.
   b. Repeat action with the other chassis ear.



2. Find the **Front** marking on the rails, and then orient the rails appropriately for attaching to the SVP chassis.
3. Screw the internal racks onto the SVP chassis using the four large screws and the two small screws.
4. Repeat steps 2 and 3 for the inner rail extension on the other side of the SVP chassis.

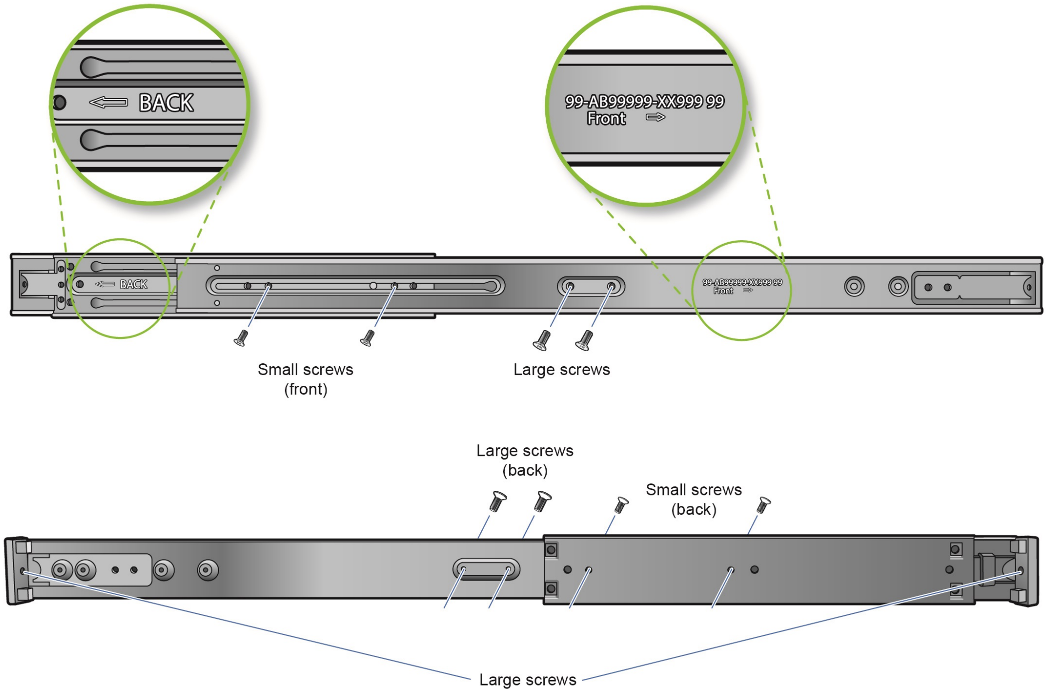
Installing the outer rails to the rack

The outer rails that secure the physical SVP directly to the rack.

Procedure

1. Attach the short bracket to the outside of the long bracket.

   You must align the pin with the slide.
2. Using the directions on the rails, orient the rails so the front of the rail faces the front of the rack. Adjust the short rail and long rail to the proper distance, so that they fit snugly into the rack. Then insert two small screws and two large M5 screws into the threaded holes in the slide area on the rails, as shown in the following figure, to prevent the rails from moving.
3. Secure the long outer rail to the vertical rail at the front of the rack using a washer and an M5 screw on one side of the rail and a safety nut on the other side. Then connect the short outer rail to the vertical rail at the rear of the rack using another washer and M5 screw.



4. Repeat steps 1 through 3 for the other outer rail.

Installing the physical SVP into the rack

After the inner and outer rails are attached to the physical SVP, the SVP can be installed in a rack.

Before you begin

Confirm the following:

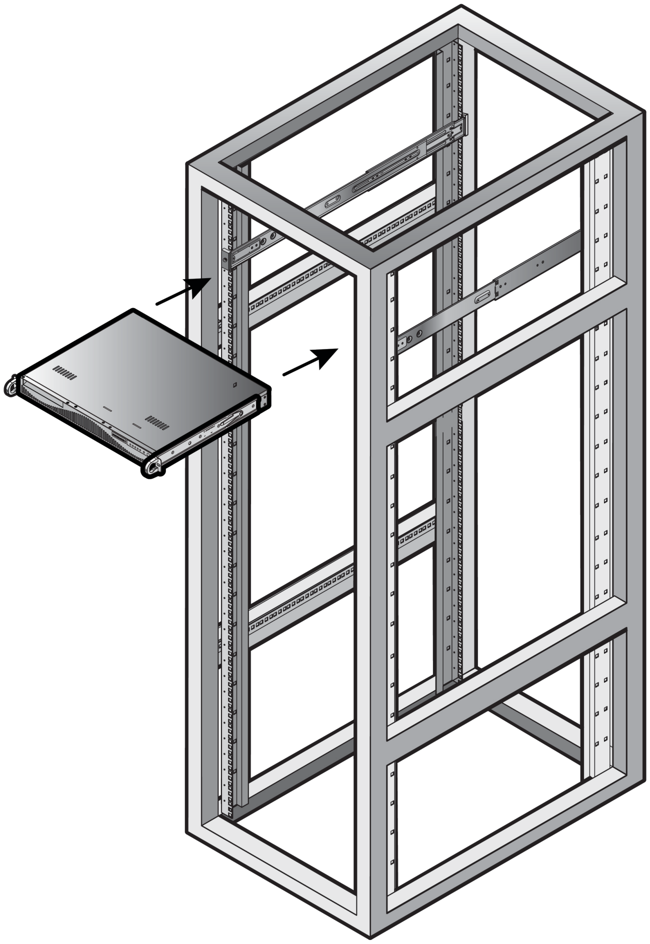
- The inner rails are attached to the SVP enclosure.
- The outer rails are attached to the rack.

Procedure

1. Align the SVP enclosure inner rails with the front of the horizontal outer rails on the rack.
2. Slide the SVP enclosure inner rails into the outer rails on the rack, keeping the pressure even on both sides.

   If necessary, press the locking tabs when inserting.

   When the SVP enclosure is pushed completely into the rack, the locking tabs snap into the locked position.



Connecting to the physical SVP

All port connections to the physical SVP are located at the rear of the SVP.

The management console must be able to access the SVP. Use Category 5 or higher Ethernet cables to connect to SVP.

> **Note:** The SVP running Windows 10 operating system does not provide an option to disable Spanning Tree Protocol (STP). If your network has BPDU enabled to prevent loops, connect the user LAN port on controllers 1 and 2 to an Ethernet switch that is also connected to the LAN1 port on the SVP.

Procedure

1. Connect the **LAN1** port to a switch on your IP network.

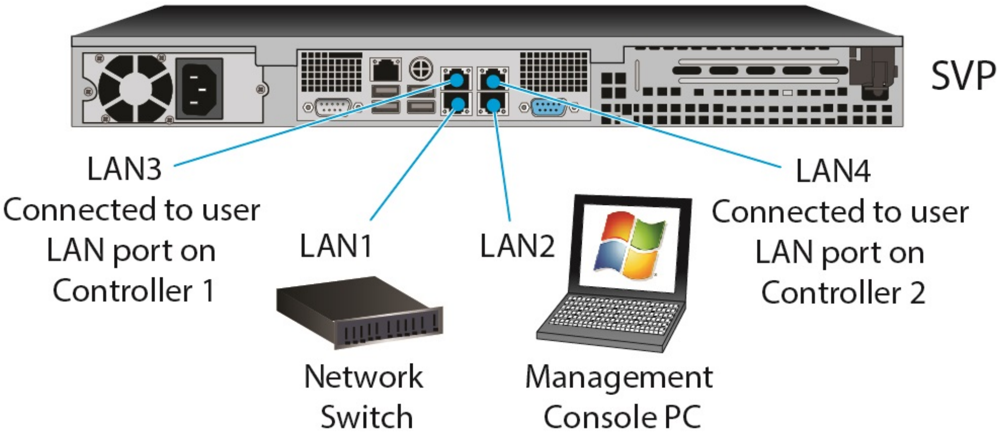
   > **Note:** If your network uses IP addresses 192.168.0.15-17, do not connect the **LAN1** port to your switch until after you complete the Initial Startup.

2. Connect the **LAN2** port to a management console PC.

   Typically, this is a notebook PC.

3. Connect the **LAN3** port to the user LAN port on storage system controller 1.

4. Connect the **LAN4** port to the user LAN port on storage system controller 2.



After you connect the physical SVP, you can set up an encrypted Secure Sockets Layer (SSL) connection between the storage system and the SVP.

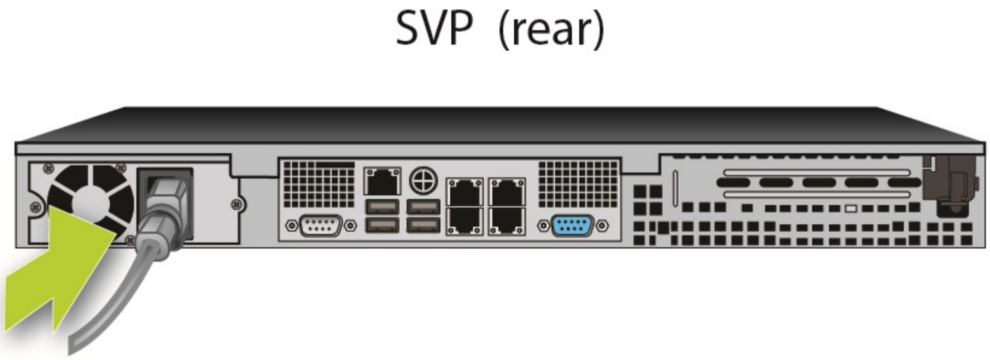
Note: Creating private and public keys requires a dedicated program, OpenSSL. OpenSSL is installed along with Storage Navigator but not allowed to be used for different purposes. To use OpenSSL for SSL communication settings, download one from the OpenSSL website (http://www.openssl.org/).

Turning on power to the physical SVP

When turning on the power to the physical SVP, use only the power cable supplied with the SVP. Do not use a power cable designed for another device.

Procedure

1. Attach the supplied power cable to the power socket on the rear panel of the physical SVP.



2. Plug the other end of the power cable into an AC power source.

   After you turn on the power, you can change the physical SVP configuration from a bridged network connection to a non-bridged network connection if BDPU guard is enabled in your networking environment.

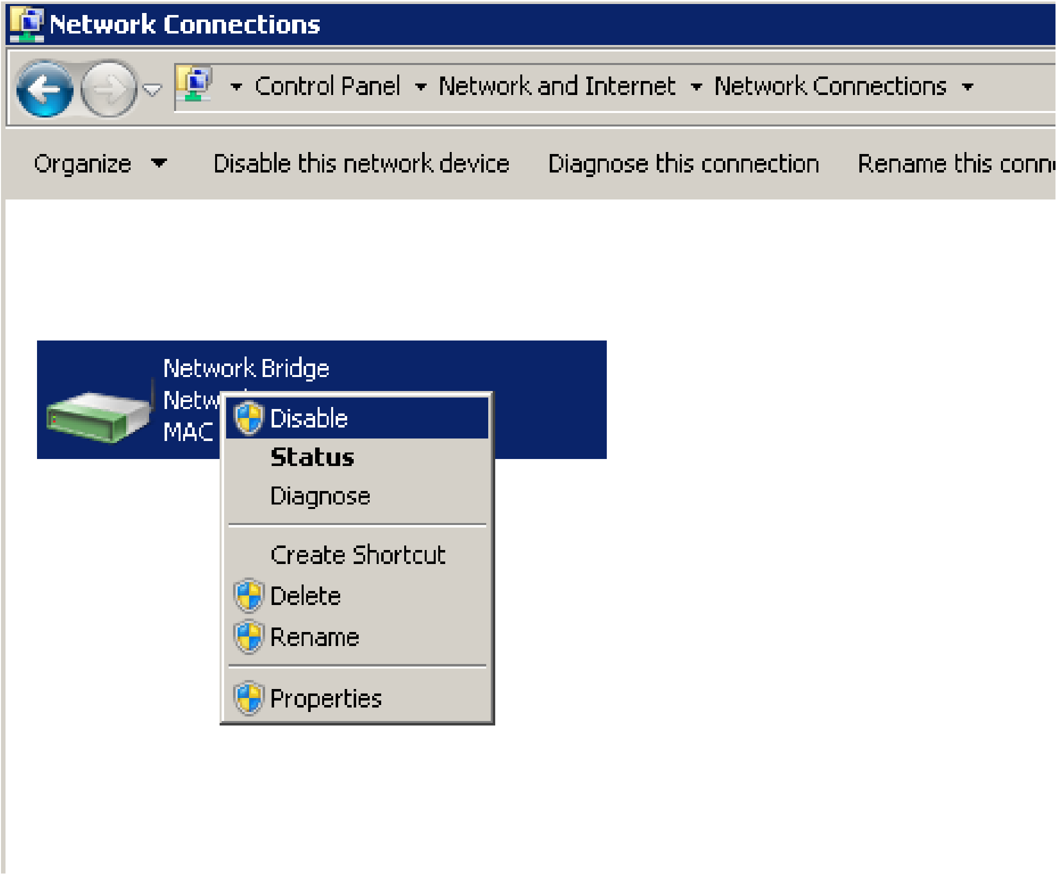
Operating the physical SVP in a non-bridged network configuration

If BPDU is enabled in your network environment, use a non-bridged configuration. This configuration disables the SVP's internal bridge, and allows you to connect the Ethernet cables from the user LAN port on CTL1 and CTL2 to an Ethernet switch.

Procedure

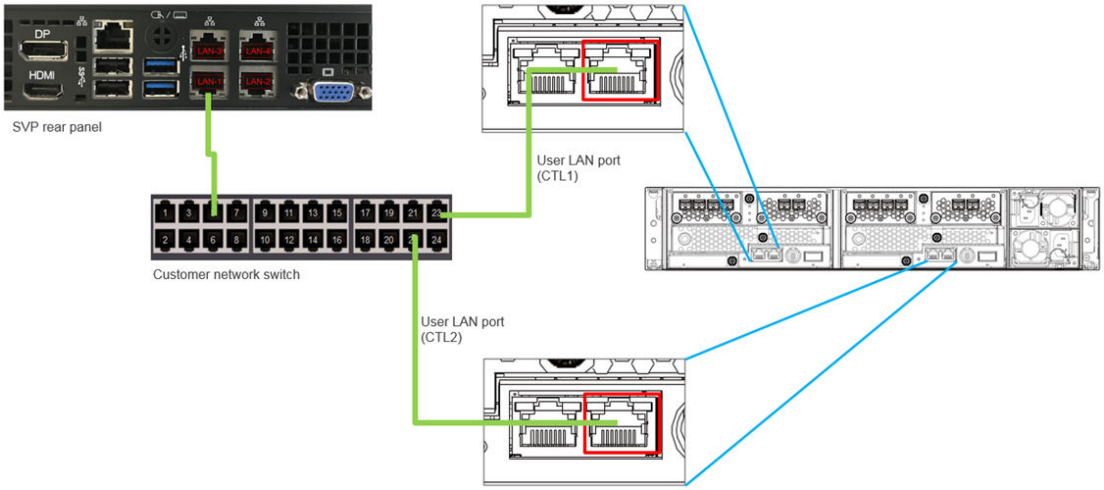
1. Connect a PC to the LAN2 port on the SVP.
2. Log on to the SVP using the Remote Desktop Connection:
   a. Configure the PC to use an IP address of 10.0.0.xxx, where xxx = 1-99 or 101-254, and a subnet mask of 255.255.255.0.
   b. Click **Start** > **All Programs**, and then select **Accessories** > **Remote Desktop Connection**.
   c. In the **Computer** field, type `10.0.0.100` and click **Connect**.
   d. In the **Windows Security** screen, type `SVP-PC\SVP` in the top field and `raid-login` in the bottom field.
   e. Click **OK**.
   f. If prompted that the identity of the remote computer cannot be verified, click **Yes** to continue.
3. In the **Remote Desktop Connection** window, select **Control Panel** > **Network and Sharing Center**.
4. Click **Change adapter settings**.
5. Right-click the network bridge icon, and then click **Disable**.

   The SVP internal bridge is now disabled.

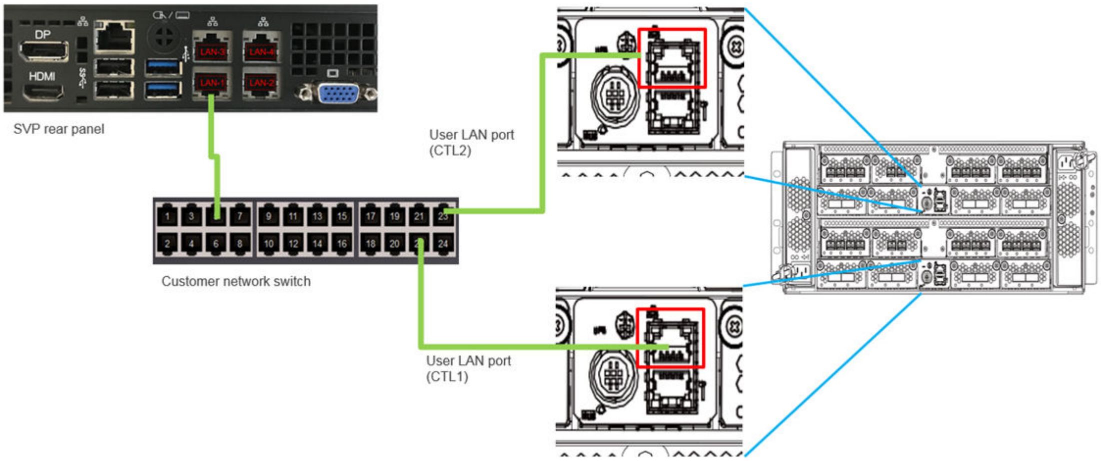


6. Remove the Ethernet cables from SVP ports LAN3 and LAN4, and attach them to the Ethernet switches.

   The following figure shows a CBSS and CBSL storage system in a non-bridged environment.



   The following figure shows a CBLM and CBLH storage system in a non-bridged environment.



Setting the SVP date, time, and time zone settings

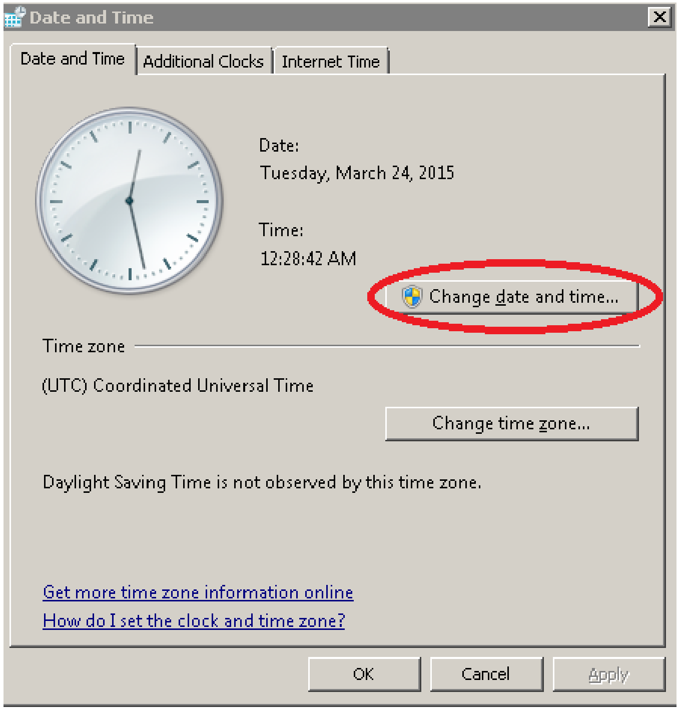
Use the management console PC to set the SVP date, time, and time zone according to the local time of the location of the installed SVP. You specify these settings using a Windows operating system running on the SVP, and then specify the same settings in the maintenance utility.

Before you begin

- Verify the management PC is connected to the LAN2 port on the SVP.
- Verify the PC establishes a Remote Desktop Connection to the SVP.
- Confirm the **Management Utility** window opens on the PC.

Procedure

1. In the desktop, click the **Start** button, and then click **Control Panel**.
2. Click **Clock, Language, and Region**.
3. Click **Date and Time**.
4. Click **Change date and time**.



Date and Time

Date:
Tuesday, March 24, 2015

Time:
12:28:42 AM

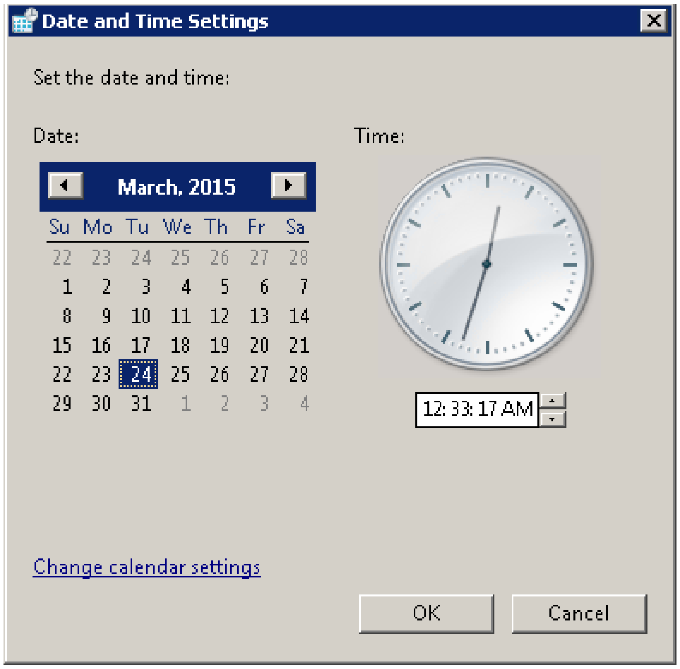
Time zone

(UTC) Coordinated Universal Time

Daylight Saving Time is not observed by this time zone.

Get more time zone information online
How do I set the clock and time zone?
OK
Cancel
Apply

5. Set the year, month, day, and time, and then click **OK**.



Date and Time Settings

Set the date and time:

Date:

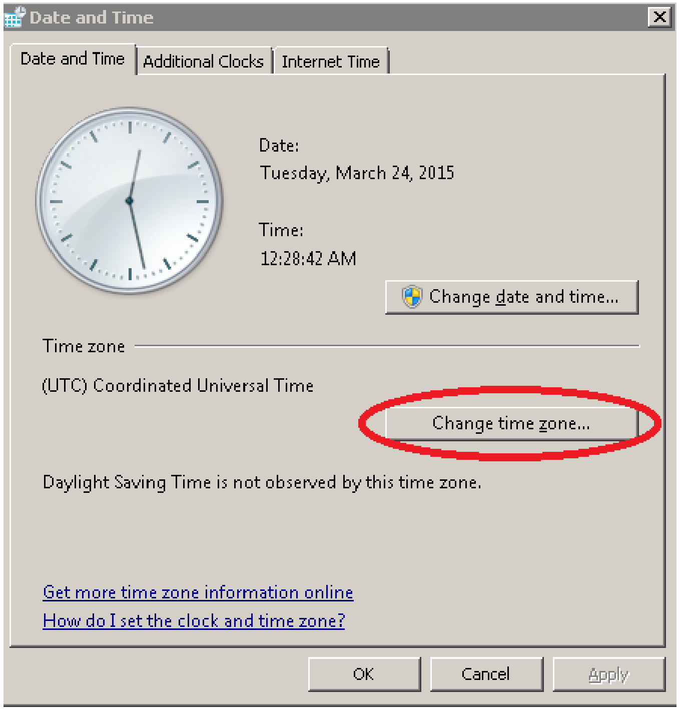
March, 2015

Su	Mo	Tu	We	Th	Fr	Sa
22	23	24	25	26	27	28
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Time:

12: 33: 17 AM

6. In the **Date and Time** tab, click **Change time zone**.



Date:
Tuesday, March 24, 2015

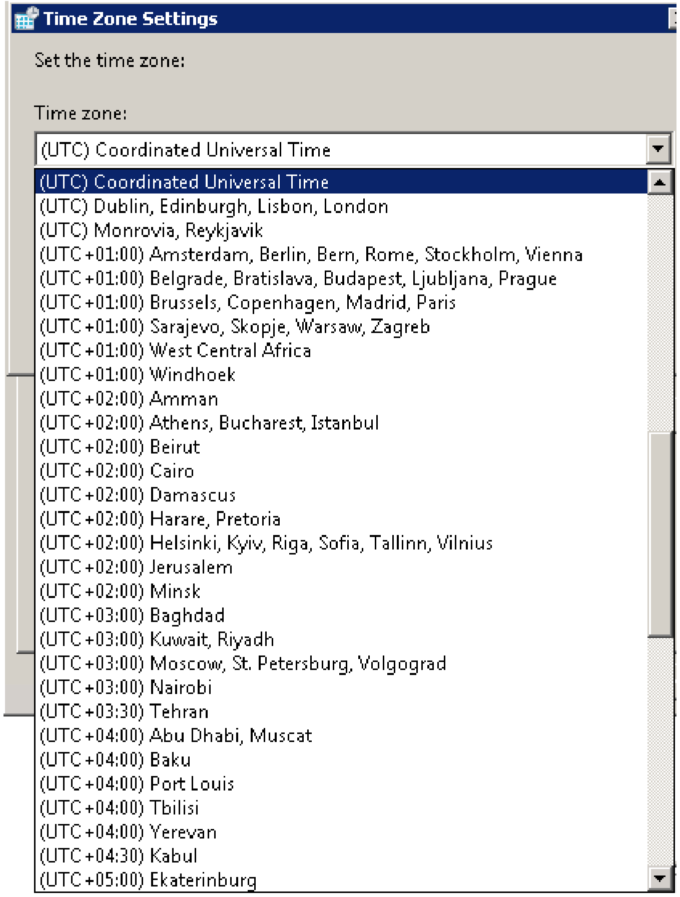
Time:
12:28:42 AM

(UTC) Coordinated Universal Time

Daylight Saving Time is not observed by this time zone.

Note: Set the SVP date, time, and time zone according to the local time of the location of the installed SVP.

7. Select a UTC time zone from the drop-down list, and then click **OK**.



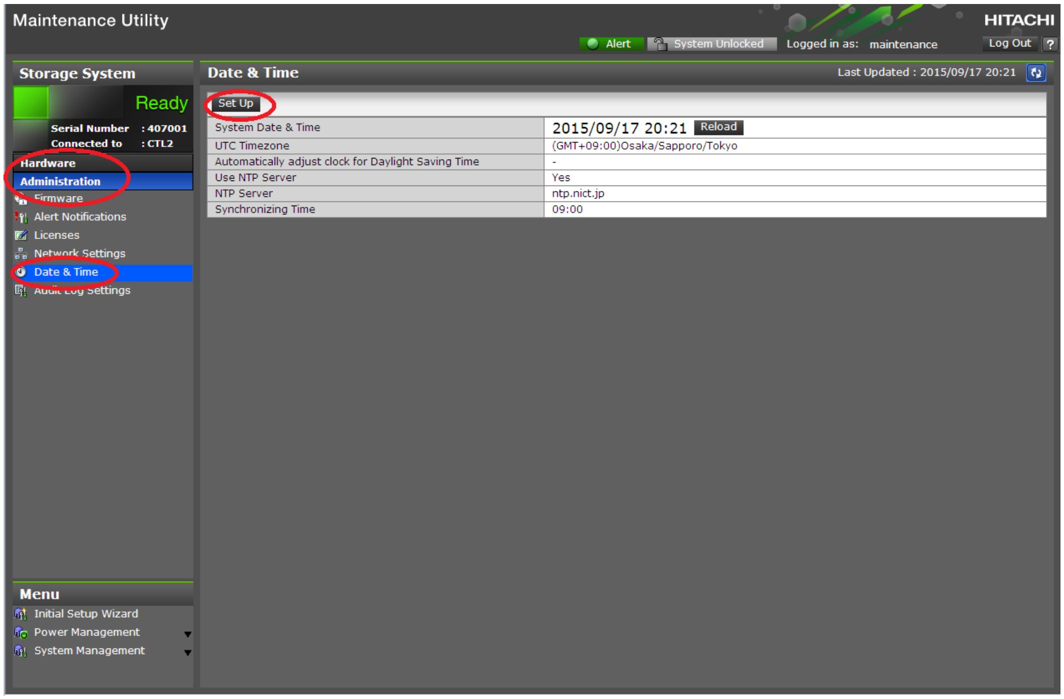
Time Zone Settings

Set the time zone:

Time zone: (UTC) Coordinated Universal Time

(UTC) Coordinated Universal Time
(UTC) Dublin, Edinburgh, Lisbon, London
(UTC) Monrovia, Reykjavik
(UTC +01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
(UTC +01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(UTC +01:00) Brussels, Copenhagen, Madrid, Paris
(UTC +01:00) Sarajevo, Skopje, Warsaw, Zagreb
(UTC +01:00) West Central Africa
(UTC +01:00) Windhoek
(UTC +02:00) Amman
(UTC +02:00) Athens, Bucharest, Istanbul
(UTC +02:00) Beirut
(UTC +02:00) Cairo
(UTC +02:00) Damascus
(UTC +02:00) Harare, Pretoria
(UTC +02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(UTC +02:00) Jerusalem
(UTC +02:00) Minsk
(UTC +03:00) Baghdad
(UTC +03:00) Kuwait, Riyadh
(UTC +03:00) Moscow, St. Petersburg, Volgograd
(UTC +03:00) Nairobi
(UTC +03:30) Tehran
(UTC +04:00) Abu Dhabi, Muscat
(UTC +04:00) Baku
(UTC +04:00) Port Louis
(UTC +04:00) Tbilisi
(UTC +04:00) Yerevan
(UTC +04:30) Kabul
(UTC +05:00) Ekaterinburg

8. Click **OK**.
9. Close the Windows Control Panel.
10. Log on to the maintenance utility.
    a. In the left pane, click **Administration** > **Date & Time**.
    b. To the right, under **Date & Time**, click **Set Up**.

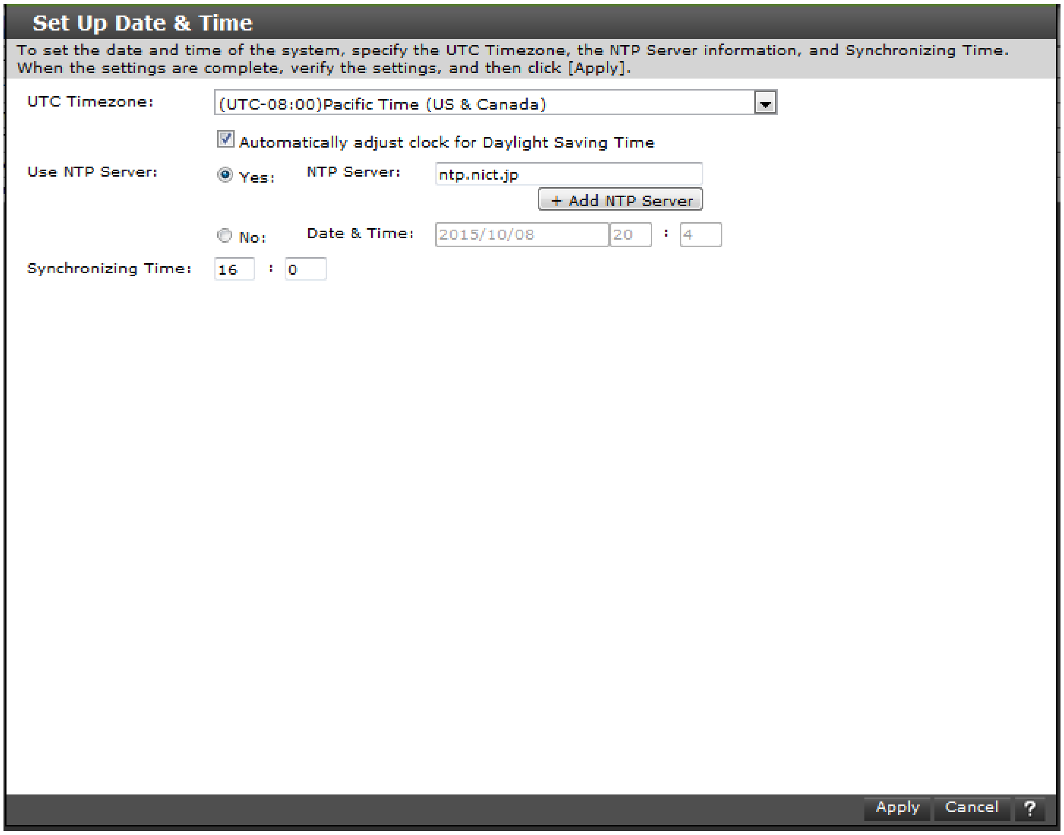


Serial Number : 407001
Connected to : CTL2

Date & Time — Last Updated : 2015/09/17 20:21

System Date & Time	2015/09/17 20:21
UTC Timezone	(GMT+09:00)Osaka/Sapporo/Tokyo
Automatically adjust clock for Daylight Saving Time	-
Use NTP Server	Yes
NTP Server	ntp.nict.jp
Synchronizing Time	09:00

c. In the **Set Up Date & Time** page, enter the date and time settings.



To set the date and time of the system, specify the UTC Timezone, the NTP Server information, and Synchronizing Time. When the settings are complete, verify the settings, and then click [Apply].

UTC Timezone: (UTC-08:00)Pacific Time (US & Canada)

☑ Automatically adjust clock for Daylight Saving Time

Use NTP Server: ● Yes: NTP Server: ntp.nict.jp

○ No: Date & Time: 2015/10/08 20 : 4

Synchronizing Time: 16 : 0

<table>
<tr><th>Field</th><th colspan="2">Description</th></tr>
<tr><td>UTC Time zone</td><td colspan="2">Select a time zone on the Coordinated Universal Time map.</td></tr>
<tr><td>Automatically adjust clock for Daylight Saving Time</td><td colspan="2">This field is available only if the selected UTC time zone supports daylight saving time. Check this option if your location observes daylight saving time (also known as summer time).</td></tr>
<tr><td rowspan="3">Use NTP Server</td><td colspan="2">Select an option for maintaining the maintenance utility time.</td></tr>
<tr><td>Yes: NTP Server</td><td>Maintenance utility time will synchronize with a Network Time Protocol (NTP) server. Enter an IP address or a server name.
- Click + Add NTP Server to add up to five NTP servers.
- Enter the IP address in IPv4 or IPv6 format.
- Enter the server name (up to 255 one-byte alphanumeric characters). Spaces can be used in the server name, but the following symbols cannot be used: !"#$%&'()*+,/;<=>?@[\]^`{|}</td></tr>
<tr><td>No: Date & Time</td><td>Set the date and time manually.
- Click the field, and then click a date from the pop-up calendar.
- Enter the minutes and seconds manually.</td></tr>
</table>

Field	Description
Synchronizing Time	To synchronize the maintenance utility time with the NTP server at a specific time, enter the synchronizing time.

d. Click **Apply**.

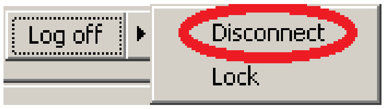
e. In the confirmation message, click **Close**.

Disconnecting the management console from the physical SVP

If you need to disconnect the management console from the physical SVP, use the following procedure.

Procedure

1. Click the **Start** button on the SVP desktop.
2. Click **Log off** > **Disconnect**.



Result

The SVP disconnects from the PC.

Chapter 5: Installing the SVP software on a customer-supplied server

The SVP provides out-of-band configuration and management of the storage system, and collects performance data for key components to enable diagnostic testing and analysis. To meet the SVP requirement for VSP Gx00 models and VSP Fx00 models, Hitachi Vantara supports bare-metal SVP installations.

Minimum requirements for installing the SVP software on customer-supplied server

Hitachi Vantara allows the SVP software to be installed on customer-supplied servers that meet the following minimum requirements.

- Processor:
  - One core with hyper-threading, two cores without hyper-threading
  - Processor performance comparable to Celeron 1.6 GHz
- Random-access memory: 3.5 GB per storage system
- Hard drive: 120 GB per storage system
- LAN connection: one 1000Base-T
- Windows 7 Professional (64-bit), Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit), Windows Server 2016, Windows 10 Professional (64-bit), or Windows 10 Enterprise (64-bit)

Note: The customer-supplied server running the Windows operating system cannot be used with the storage system if it belongs to different subnets, and if a router or a firewall is filtering packets according to a defined condition. There is not a limit for distance between the server running the SVP application and storage array being managed if they belong to the same subnet.

Setting up the SVP locale

The SVP and storage management software support the English and Japanese languages.

If you intend to install the SVP software using a language other than English and Japanese, change the SVP's locale setting to reflect the appropriate language using the procedure for the Windows version installed on the SVP. For more information, see the instructions for your Windows operating system.

Configuring the operating system

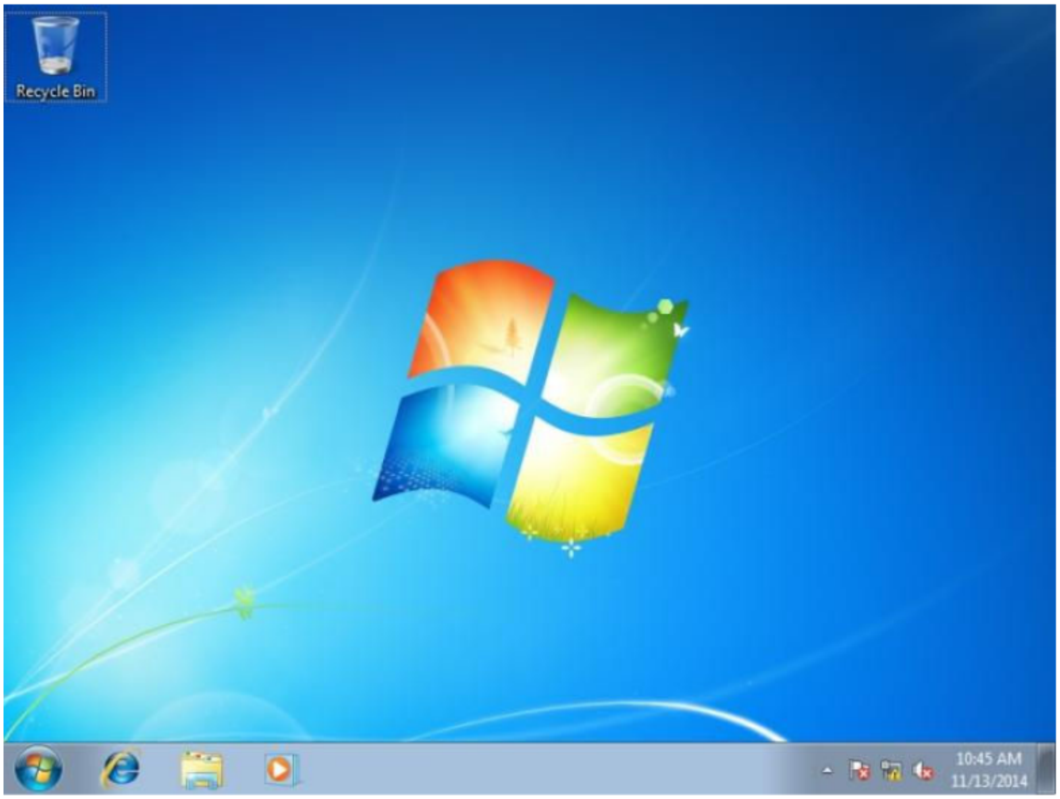
The SVP runs on a customer-supplied version of Windows 7 Professional (64-bit), Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit), Windows Server 2016 (64-bit), Windows 10 Professional (64-bit), or Windows 10 Enterprise (64-bit) .

The following procedures describe how to configure the Windows 7 Professional (64-bit) operating system on the customer-supplied server. These procedures assume that the operating system has already been installed on the server.

Logging on to the operating system

The log on procedure is performed using the Windows operating system installed on the SVP.

Using the Remote Desktop Connection, log on as the user who was specified during the Windows installation (for example, `Administrator`).



Next steps

Configure the Control Panel display.

Configuring the Control Panel display

Procedure

1. Open the Control Panel.
2. From the **View by** list, select **Large icons**.

   Note: After configuring the control panel display, configure the desktop.

Configuring the desktop

Configure the Windows screen saver function on the SVP.

Procedure

1. Click **Control Panel** > **Personalization**. For **Basic and High Contrast Themes (6)**, click **Windows Classic**.
2. Click **Screen saver**.
3. In **Screen saver**, click **Blank**, and then set **Wait** to **60 (minutes)**.
4. Click **OK**.

Next steps

Configure the task bar and the start menu properties.

Configuring the task bar and the start menu properties

Configure the Taskbar and Start menu properties on the Windows operating system running on the SVP.

Procedure

1. Click **Control Panel** > **Taskbar and Start Menu Properties (task bar property)**, and then click the **Taskbar** tab.
2. Click **Customize**.
3. In the **Notification Area Icons** window, check **Always show all icons and notifications on the taskbar**.
4. Click **OK**.
5. Click **Control Panel** > **Taskbar and Start Menu Properties (task bar property)**, and then click the **Start Menu** tab.
6. Click **Customize**.
7. In the **Customize Start Menu** window, check **Run command** and click **Display on the All Programs menu and the Start menu**.
8. Under **Music**, check **Don’t display this item**.
9. Click **OK**.
10. In the **Taskbar and Start Menu Properties** window, click **OK**.

Note: After configuring the Task bar and Start Menu properties, configure the time settings.

Configuring the time settings

Configure the SVP for Universal Coordinated Time, and then configure it to not synchronize with an Internet time server.

Procedure

1. Click **Control Panel** > **Date and Time**, and then click the **Date and Time** tab.
2. Click **Change time zone**.
3. In the **Time Zone Settings** window, click **(UTC) Coordinated Universal Time**, and then click **OK**.
4. Click **Control Panel** > **Date and Time**, and then click the **Internet Time** tab.
5. Click **Change settings**. In the **Internet Time Settings** window, uncheck **Synchronize with an Internet time server**, and then click **OK**.
6. In the **Date and Time** window, click **OK**.

Note: After configuring the time settings, configure the region settings.

Configuring region settings

Configure the region and language the language for your region or preference.

Procedure

1. Click **Control Panel** > **Region and Language**, and then click the **Keyboards and Languages** tab.
2. Click **Change keyboards**.
3. In the **Text Service and Input Languages** window, click the **Language Bar** tab.
4. Click **Hidden**, and then click **OK**.
5. Click **Control Panel** > **Region and Language**, and then click the **Administrative** tab.
6. Click **Change system locale**.
7. In the Region and Language settings window, for **Current system locale**, select the language for your region or preference.
8. Click **OK**.
9. In the **Change System Locale** window, click **Restart now**.
10. After the restart, click **Control Panel** > **Region and Language**, and then click the **Keyboards and Languages** tab.
11. Click **Change Keyboards**, and then click the **General** tab.
12. In the **Text Services and Input Languages** window, if **Japanese(Japan)** appears under **Installed services**, click the current selection, and then click **Remove**.
13. Click **OK**.

14. In the **Region and Language** window, click **OK**.

> **Note:** After configuring the region settings, configure the power management settings.

Configuring the power management settings

For optimum performance, the SVP requires specific power management settings.

Procedure

1. Click **Control Panel** > **Power Options**, and then click the **Show additional plans** list.
2. Click **Change settings that are currently unavailable**.
3. Click **High Performance** and **Change plan settings**.
4. In the **Edit Plan Setting** window, click **Change settings that are currently unavailable**.
5. In **Turn off the display**, select **Never**, and then click **Change advanced power settings**.
6. In the **Advanced settings** tab of the **Power Options** window, click **Change settings that are currently unavailable**. Then click **Hard disk** > **Turn off hard disk after**, and select **Never**.
7. Click **Processor power management** > **Minimum processor state**, and then select `5`.
8. Click **OK**.
9. In the **Edit Plan Setting** window, click **Save change**, and then close the window.

> **Note:** After defining the power management settings, configure the Action Center settings.

Configuring Action Center settings

All settings in the Windows Action Center must be disabled.

Procedure

1. Click **Control Panel** > **Action Center**, and then click **Change Action Center settings**.
2. In the **Change Action Center settings** window, clear all the items, click **OK**, and then close the window.

> **Note:** After configuring Action Center settings, configure the troubleshooting settings.

Configuring the troubleshooting settings

The Windows Computer Maintenance setting must be disabled.

Procedure

1. Click **Control Panel** > **Troubleshooting**, and then click **Change settings**.
2. In the **Change settings** window, for **Computer Maintenance**, click **Off**, and clear all configuration options below **Other settings**.
3. Click **OK**, and then close the window.

> **Note:** After configuring the troubleshooting settings, configure the Remote Desktop settings.

Configuring the Remote Desktop settings

Remote access to the SVP is required and appropriate Windows firewall settings must be configured.

Procedure

1. Click **Control Panel** > **System**, and then click **Remote settings**.
2. In the **System Properties** window, click the **Remote** tab.
3. Under **Remote Assistance**, clear **Allow Remote Assistance connections to this computer**.
4. Under **Remote Desktop**, click **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**.
5. Click **OK**.
6. If a message states that the Remote Desktop Firewall will be enabled, click **OK**.
7. Click **OK** to close the **System Properties** window.
8. Close the **System** window.
9. Click **Control Panel** > **Windows Firewall**, and then click **Allow a program or feature through Windows firewall**.
10. Click **Change settings**, and then verify **Remote Desktop** and **Remote Desktop - RemoteFX** for both **Home/Work (Private)** and **Public** are selected.
11. Click **OK**.
12. Close the **Windows Firewall** window.

> **Note:** After configuring the Remote Desktop settings, configure the Internet Explorer settings.

Configuring Internet Explorer settings

Configure Internet Explorer advanced, security, and properties settings.

Procedure

1. Click **Control Panel** > **Internet Options**, and then click the **Advanced** tab to modify the settings.
2. Under **Security**, select **Allow active content to run in files on My Computer**.
3. Clear **Use SSL 3.0**.

4. If **SSL 2.0** is selected, clear it.
5. Select **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2**.
6. Click **OK**.
7. Close the **Internet Properties** window.
8. From the **Control Panel** window, click **System and Security** > **Action Center**.
9. If the **SmartScreen Filter** window appears, click **OK**.
10. Click **All Programs** > **Internet Explorer**.
11. If the **Set Up Windows Internet Explorer 8** window appears, click **Next**.
12. In the **Turn on Suggested Sites** window, click **No, don't turn on**, and then click **Next**.
13. In the **Choose your settings** window, click **Use express settings**, and then click **Finish**.
14. When an error indicates that an Internet connection is not established, close Internet Explorer.

Note: After configuring Internet Explorer settings, disable the auto-execute feature.

Disabling the auto-execute feature

The SVP requires the Windows AutoPlay feature be turned off.

Procedure

1. Click **Start** > **Run**, and then type `gpedit.msc` to start the Group Policy Editor.
2. Click **Local Computer Policy** > **Computer Configuration**, click **Administrative Templates** > **Windows Components**, and then click **AutoPlay Policies**.
3. From the items on the right, double-click **Turn off Autoplay**.
4. In the **Property** window, click **Enabled** and select **All drives**, and then click **OK**.
5. Close the Group Policy Editor.
6. Click **Control Panel** > **Autoplay**.
7. Clear **Use Autoplay for all media and devices**, and then click **Save**.

Note: After disabling the auto-execute feature, configure the Registry.

Configuring the Registry

Use Regedit to edit the Windows Registry on the SVP.

Procedure

1. Disable anonymous logon (null connection):
   a. Click **Start** > **Run**, and then type `regedit` and press **Enter**.
   b. In the **User Account Control** menu, click **Yes** to open the **Registry Editor** window.

   c. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
   d. Double-click **restrictanonymous**.
   e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.

2. Disable the beep when Remote Desktop Connection is connected:
   a. In the **Registry Editor** window, navigate to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server`.
   b. In the **Edit** menu, click **New** > **DWORD (32-bit) Value**.
   c. Type `DisableBeep`.
   d. Double-click **DisableBeep**.
   e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.
3. Configure Remote Desktop Connection:
   a. In the **Registry Editor** window, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services`.
   b. In the **Edit** menu, click **New** > **DWORD (32-bit) Value**.
   c. Type `fPromptForPassword`.
   d. Double-click **fPromptForPassword**.
   e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.
   f. In the **Edit** menu, click **New** > **DWORD (32-bit) Value**.
   g. Type `SecurityLayer`.
4. Restart the server.

   Note: After configuring the Registry, enable ICMP (ping) reply.

Enabling ICMP (ping) reply

The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. The protocol is used by network devices, such as routers, to send error messages and operational information indicating, as an example, a requested service is not available or a host or router could not be reached.

Procedure

1. Click **Control Panel** > **Administrative Tools**, and then start **Windows Firewall with Advanced Security**.
2. In the left pane, click **Inbound Rules**.
3. Click all the following inbound rules, and then right-click and click **Enable Rules**.
   - File and Printer Sharing (Echo Request - ICMPv4-In) (Profile=Domain)
   - File and Printer Sharing (Echo Request - ICMPv4-In) (Profile=Private)
   - File and Printer Sharing (Echo Request - ICMPv6-In) (Profile=Domain)
   - File and Printer Sharing (Echo Request - ICMPv6-In) (Profile=Private)

Note: After enabling ICMP (ping) reply, change the computer name.

Changing the computer name

Changing the computer name allows the SVP to be identified easily.

Procedure

1. Click **Control Panel** > **System**, and then click **Change settings** under **Computer name, domain, and workgroup settings**.
2. In the **System Properties** window, click the **Computer Name** tab, and then click **Change**.
3. In the **Computer Name** field, type `SVP-PC`.
4. When prompted to restart your computer, click **OK**.
5. Click **Close**.
6. Click **Restart Now**.
7. Wait for the server to restart.

Note: After changing the computer name, change the account name.

Changing the account name

The following user names might differ from the user name that was specified during the Windows installation.

Procedure

1. Click **Control Panel** > **User Accounts**, and then click **Change your account name**.
2. Type `SVP` for the new account name, and then click **Change Name**.
3. Close the **User Accounts** window.
4. Click **Control Panel** > **Administrative Tools**, and then click **Computer Management**.
5. Click **Computer Management (Local)** > **System Tools**, and then click **Local Users and Groups** > **Users**.
6. In the right window, right-click **User**, and then click **Rename**.
7. Rename **User** to **SVP**.
8. Close the **Computer Management** window, and then close the **Administrative Tools** window.

Note: After changing the account name, configure the password setting for the Administrator.

Configuring the password setting for Administrator

The Windows Administrator password must be configured for use with the SVP.

Procedure

1. Click **Control Panel** > **Administrative Tools**, and then click **Computer Management**.
2. Click **Computer Management (Local)** > **System Tools**, and then click **Local Users and Groups** > **Users**.
3. In the right window, right-click **Administrator**, and then click **Set Password**.
4. In the warning message, click **Proceed**.
5. In the **New password** and **Confirm password** fields, type the administrator password `raid-login`.
6. Click **OK**.
7. Close the **Computer Management** window, and then close the **Administrative Tools** window.
8. Restart Windows.

> **Note:** After configuring the password setting for Administrator, change the password setting.

Changing the password setting

Change the password for the Windows operating system running on the SVP.

Procedure

1. Click **Control Panel** > **User Accounts**.
2. Click **Create a password for your account**.
3. In the top two fields, type the password `raid-login`. Leave the password hint field empty.
4. Click **Create password**.
5. Close the window.

> **Note:** After changing the password setting, install the SVP software.

Configuring Internet Information Services

Internet Information Services (IIS) is an extensible web server created by Microsoft for use with Windows operating systems.

Procedure

1. Click the Start button, and then click **Control Panel**.
2. Click **Programs and Features** > **Turn Windows Features On or Off**.
3. Expand **Internet Information Services**.

4. Check the following check boxes:
   - **FTP Server**
     - **FTP Extensibility**
     - **FTP Service**
   - **Web Management Tools**
     - **IIS 6 Management Compatibility**
     - **IIS 6 Scripting Tools**
     - **IIS 6 WMI Compatibility**
     - **IIS Metabase and IIS 6 configuration compatibility**
     - **IIS Management Console**
     - **IIS Management Scripts and Tools**
     - **IIS Management Service**
5. Uncheck **World Wide Web Services**.

Next steps

Install the SVP software.

Installing the SVP software

You install the SVP software from the SVP ISO image for your storage system. This image is part of the microcode distribution set and has the file name **`H8-SVP-XXX-XX.iso`**.

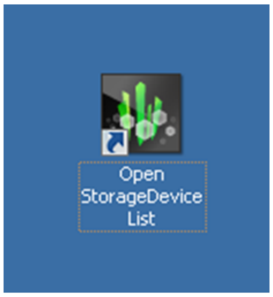
Procedure

1. Obtain the appropriate SVP ISO image for your storage system from the firmware distribution set. Verify the ISO image corresponds to the firmware currently running on the storage system.
2. Download the SVP ISO from TISC to the CE notebook, and then use an ISO reader to mount the SVP ISO as the next available drive letter.
3. Launch Remote Desktop Connection and click the **Show Options** drop-down menu.
4. Click the **Local Resources** tab, and then click **More**.
5. Expand **Drives**, and then check the drive that has the ISO.
6. Click **Connect**.
7. When prompted to enter your credentials, enter your SVP password and click **OK**.

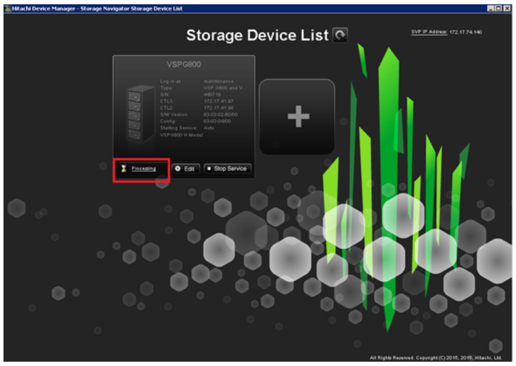
8. Perform the appropriate step:
   - If you have WinZip installed on the VM, extract the ISO locally, and then go to step 9 to run the setup application.
   - Otherwise, click the mapped drive in the left pane and double-click the **Setup** application in the workspace to the right of the pane (see the following figures), and then go to step 9.

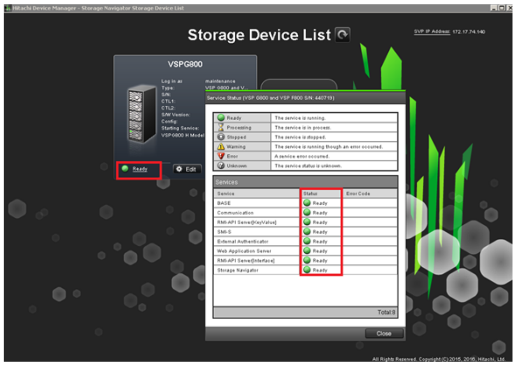
   > **Note:** Using WinZip is the preferred method. The alternative method performs the installation over the network and can take significantly longer to complete.

9. In the **Windows Security Alert** window, select **Private networks, such as my home or work network**. Then clear **Public networks, such as those in airports and coffee shops (not recommended because the networks often have little or no security)**.
10. Type the SVP IP address.
11. Click **Apply**.
12. Add the storage system.
13. Register the storage system.
14. Click the storage system.
    You are presented with the following two options:
    - Upgrading the firmware and adding the storage system
    - Adding the storage system without upgrading the firmware
15. If the storage system firmware is current, click **Select Update Objects** and clear **Firmware (Storage System)**. Doing so adds the storage system without upgrading the firmware.
16. Click **Apply**, and then click **Confirm** to added the storage system to the SVP.
17. On the Desktop, click the **Open StorageDevice List** shortcut.



Wait 10-15 minutes for all the services to start.


Hitachi Device Manager - Storage Navigator Storage Device List
Storage Device List
VSPG800
Processing
Edit
Stop Service



Service Status (VSP G800 and VSP F800 S/N: 440719)

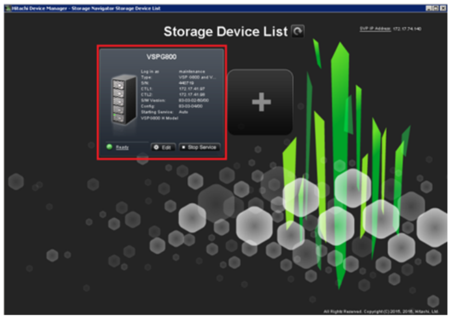
Ready	The service is running.
Processing	The service is in process.
Stopped	The service is stopped.
Warning	The service is running though an error occurred.
Error	A service error occurred.
Unknown	The service status is unknown.

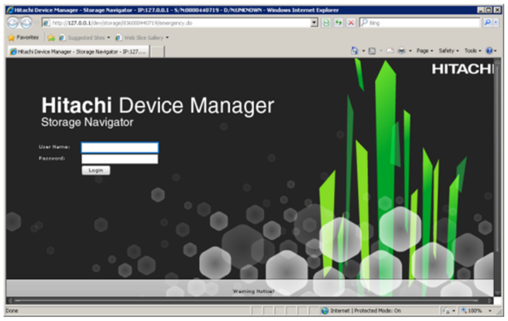
Services

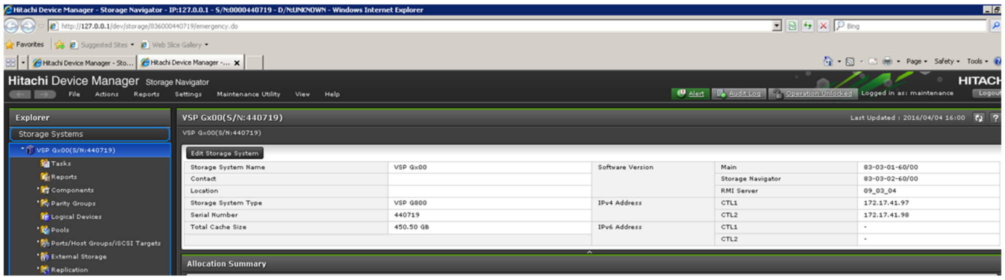
Service	Status	Error Code
BASE	Ready	
Communication	Ready	
RMI-API Server[KeyValue]	Ready	
SMI-S	Ready	
External Authenticator	Ready	
Web Application Server	Ready	
RMI-API Server[Interface]	Ready	
Storage Navigator	Ready	

Total:8

18. After the services are ready, click the storage system to start Hitachi Device Manager - Storage Navigator.







VSP Gx00(S/N:440719) Last Updated : 2016/04/04 16:00

Storage System Name	VSP Gx00	Software Version	Main	83-03-01-60/00
Contact			Storage Navigator	83-03-02-60/00
Location			RMI Server	09_03_04
Storage System Type	VSP G800	IPv4 Address	CTL1	172.17.41.97
Serial Number	440719		CTL2	172.17.41.98
Total Cache Size	450.50 GB	IPv6 Address	CTL1	-
			CTL2	-

Chapter 6: Installing the SVP software on an Oracle Linux KVM host

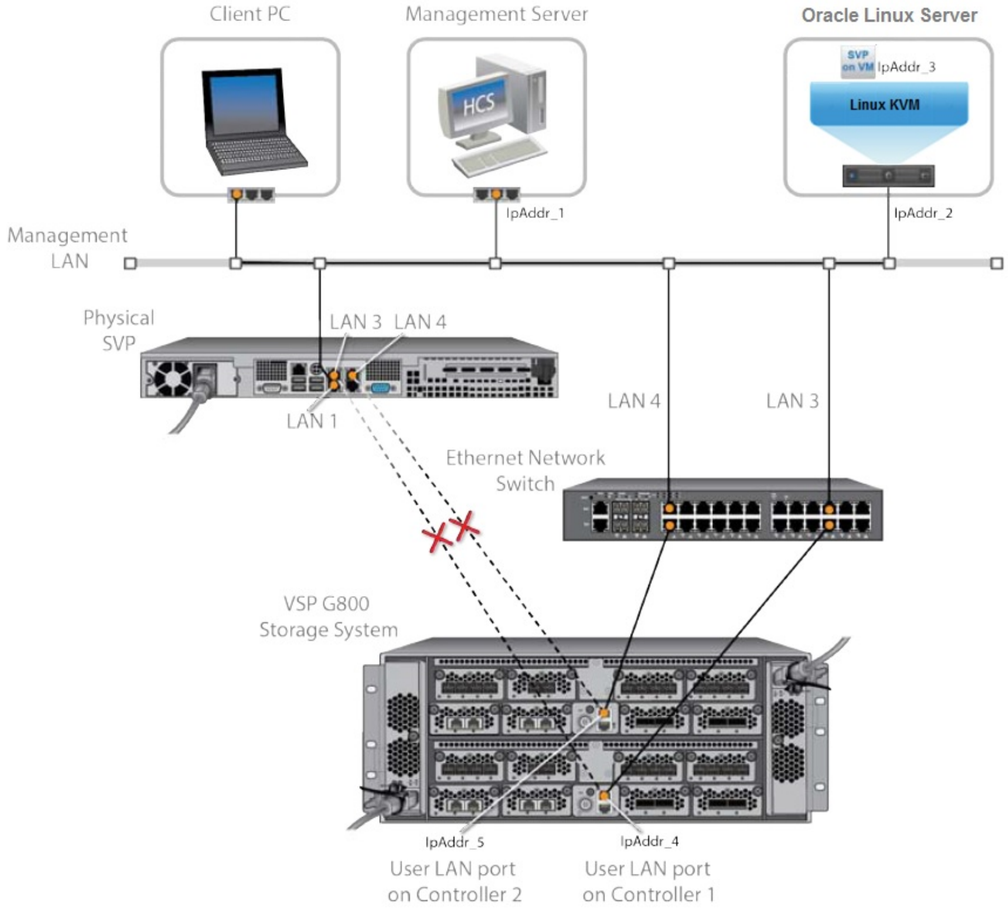
Hitachi Vantara supports configurations where a single SVP communicates with a single VSP Gx00 or VSP Fx00 model. This configuration can coexist with, or replace, all other physical, virtual, and bare-metal SVP configurations.

Physical network connection for an Oracle Linux KVM-based SVP

SVP and storage system connections are performed using the ports on the back of these devices.

The following figure shows the physical network connection for an Oracle Linux KVM-based SVP configuration using the Hitachi Virtual Storage Platform G800. Adjust your connections appropriately if you use different VSP Gx00 models or VSP Fx00 models.

Note: The Oracle Linux KVM server running the VM instance cannot be used with the storage system if it belongs to different subnets, and if a router or a firewall is filtering packets according to a defined condition. There is no distance limit between the server running the SVP application and the storage array being managed if they belong to the same subnet.



Note: In this figure, the HCS instance can also run as a VM instance.

Minimum requirements for an Oracle Linux KVM SVP

Using an SVP in an Oracle Linux KVM environment must meet the following minimum requirements.

Prerequisites

Linux KVM Server (provided by the customer)

- Oracle Linux 7.x server
- Two quad core processors, Intel Xeon 2.29 GHz
- One-port NIC
- SVP guest OS
- 128-GB RAM

SVP Guest OS (1 DKC) (maximum 1 DKC per SVP guest OS)

- Two vCPUs
- One virtual network adapter
- 4-GB RAM
- 120-GB disk space
- Windows 7 Professional (64-bit) or Windows 10 IoT Enterprise

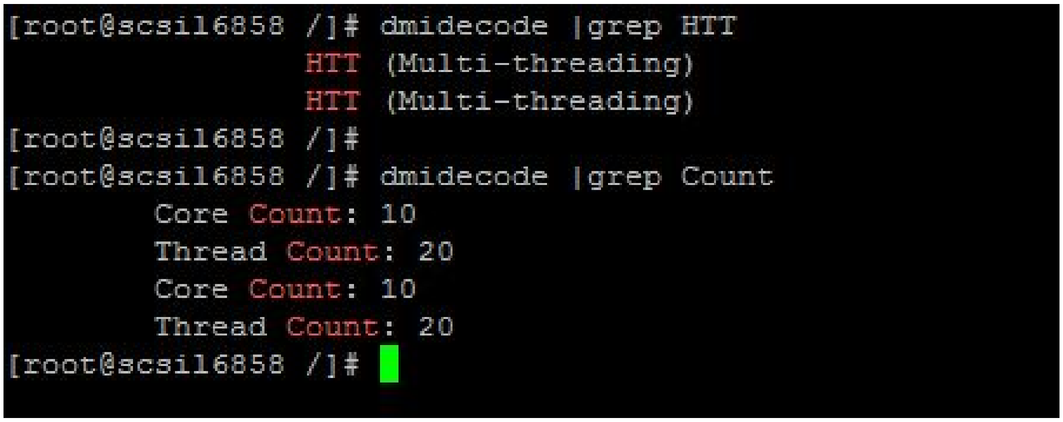
Miscellaneous

- WinZip

Hyper-threading

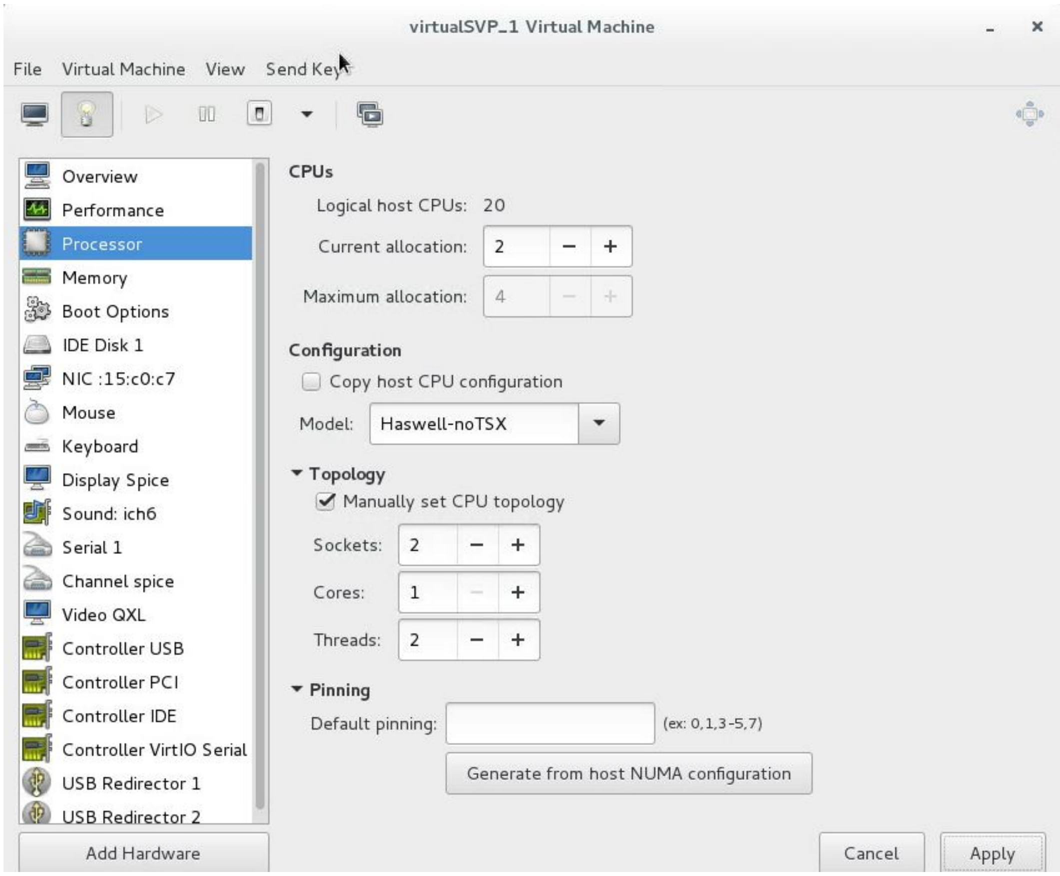
Verify that hyper-threading is active for the Oracle Linux KVM server and VM guest host. (Hyper-threading is enabled by default.)

The following figure shows an example of hyper-threading on an Oracle Linux KVM server.



```
[root@scsil6858 /]# dmidecode |grep HTT
                HTT (Multi-threading)
                HTT (Multi-threading)
[root@scsil6858 /]#
[root@scsil6858 /]# dmidecode |grep Count
        Core Count: 10
        Thread Count: 20
        Core Count: 10
        Thread Count: 20
[root@scsil6858 /]#
```

The following figure shows an example of hyper-threading on a VM guest host.



CPUs

Logical host CPUs: 20

Current allocation: 2

Maximum allocation: 4

Configuration

□ Copy host CPU configuration

Model: Haswell-noTSX

Topology

☑ Manually set CPU topology

Sockets: 2

Cores: 1

Threads: 2

Pinning

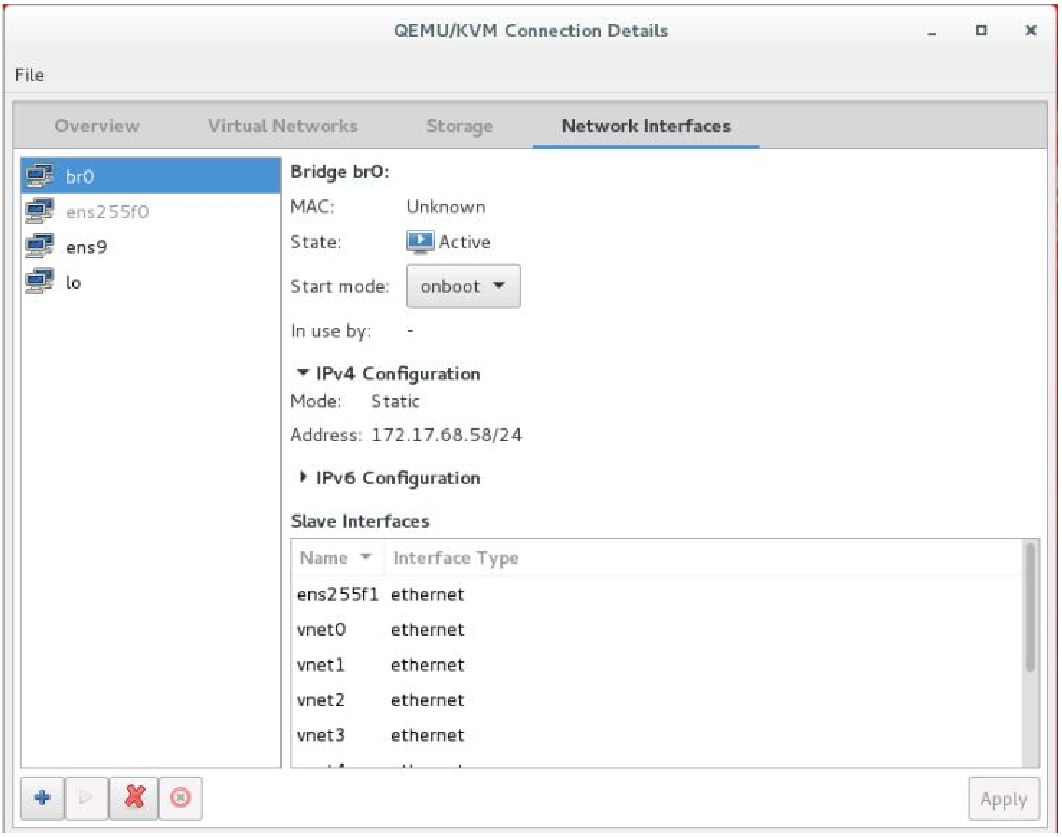
Default pinning: (ex: 0,1,3-5,7)

Configuring the Oracle Linux KVM-based SVP

After preparing the environment, activating hyper-threading on both the Oracle Linux KVM server and VM guest host, and verifying the configuration layout, configure the SVP in the Oracle Linux KVM environment.

Procedure

1. On the Oracle Linux KVM host, create a VM that is appropriate for the Windows operating system being used.
2. Verify that the virtual network connection is properly assigned to the appropriate virtual machine network.



Bridge br0:

MAC: Unknown

State: Active

Start mode: onboot

In use by: -

IPv4 Configuration

Mode: Static

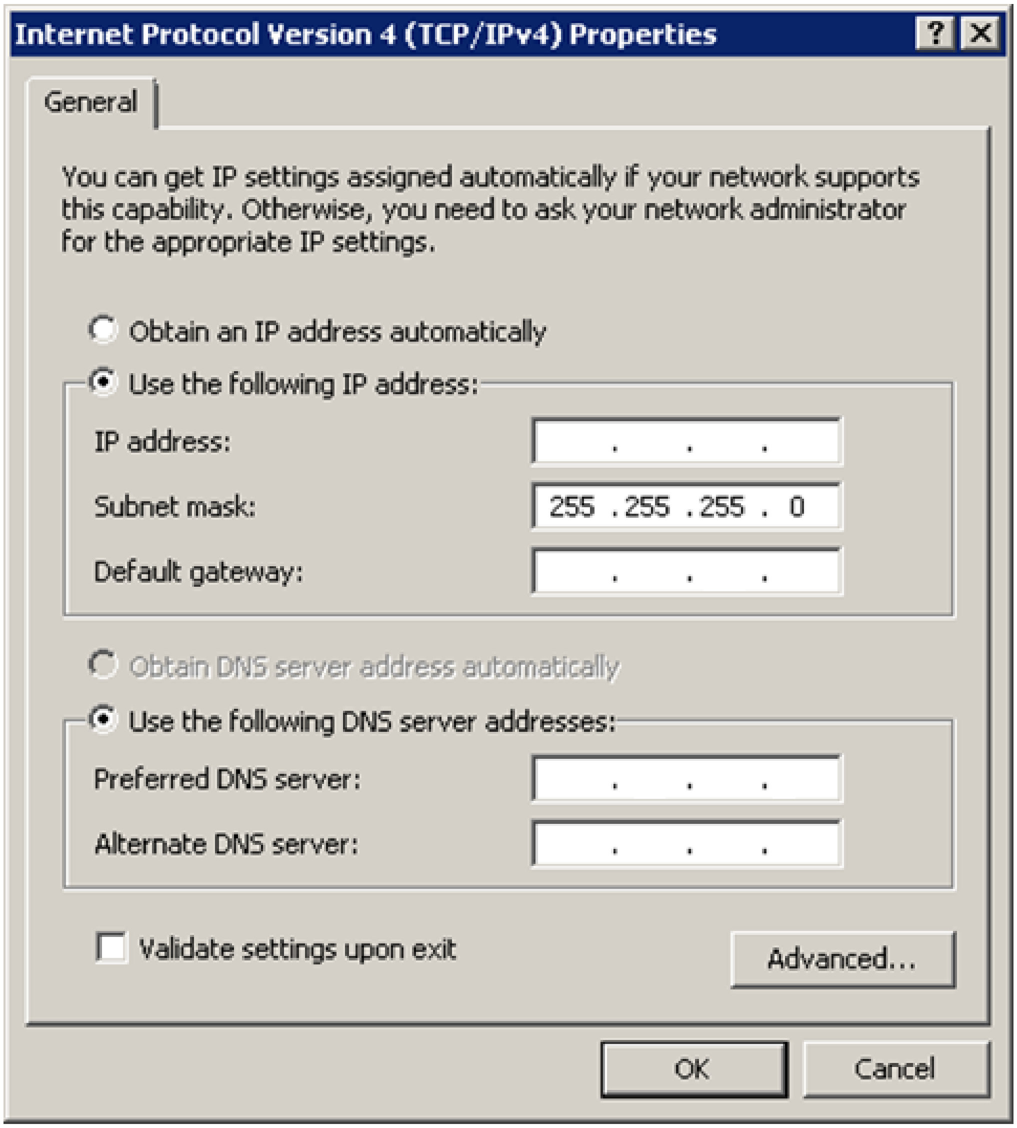
Address: 172.17.68.58/24

IPv6 Configuration

Slave Interfaces

Name	Interface Type
ens255f1	ethernet
vnet0	ethernet
vnet1	ethernet
vnet2	ethernet
vnet3	ethernet

3. Configure the network settings for the VM. The IP address must allow communication with the storage system controllers.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

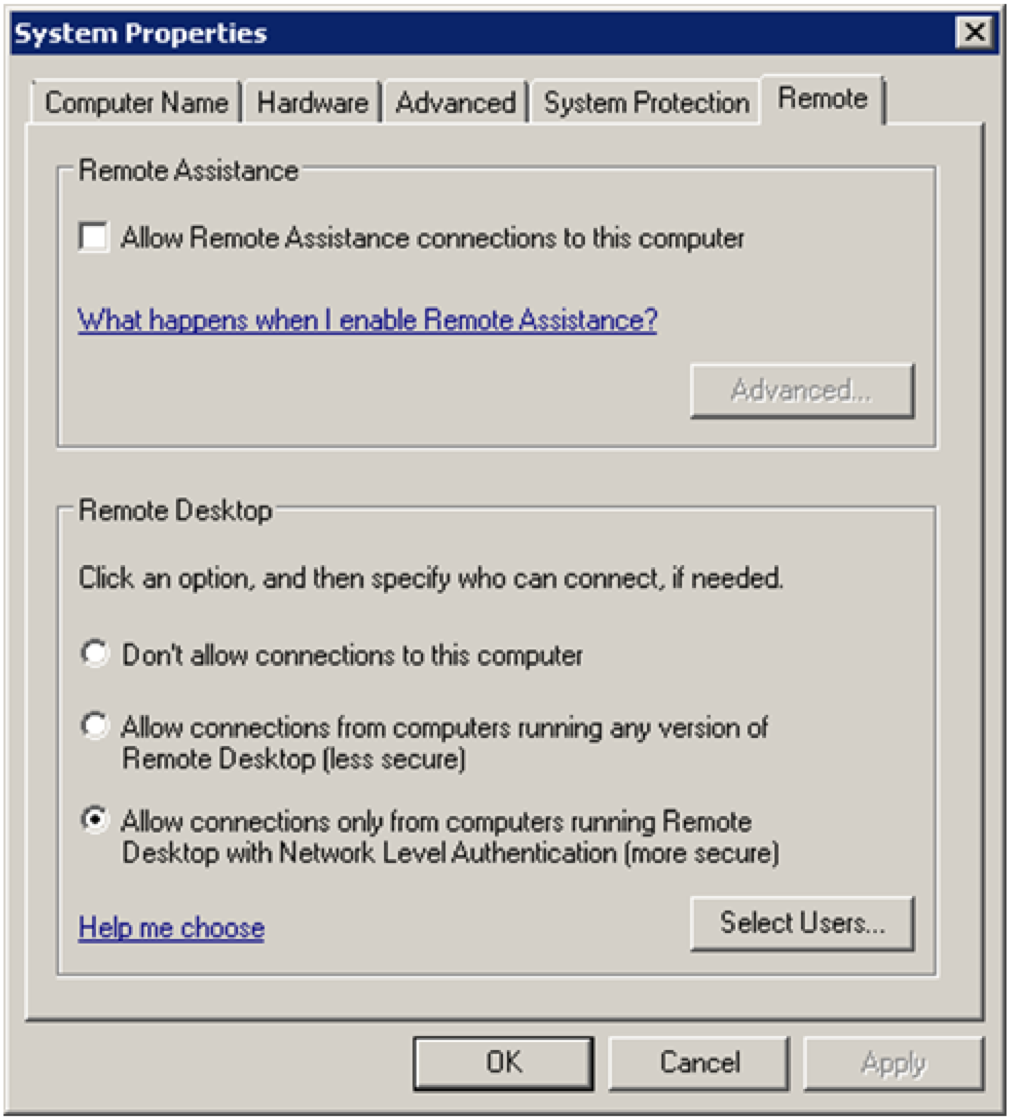
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

4. Configure a Remote Desktop connection.



Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

● Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Where to go from here

To complete the installation, perform the following steps. For details, refer to the equivalent instructions for installing the SVP on a VMware ESXi host.

Procedure

1. Configure the SVP guest OS.
2. Install the SVP software.
3. Deploy a cloned virtual SVP (optional).
4. Change the locale setting if the currently configured language is not appropriate.

Chapter 7: Installing the SVP software on a VMware ESXi host

You can use a virtual SVP with the VSP Gx00 models and VSP Fx00 models. The virtual SVP is a software application that runs on either Windows 7 Professional x64 (64-bit) on a VMware ESXi 6.0.0 host or on Windows 7 Professional Service Pack 1 (64-bit) on a VMware ESXi 6.0 U2 host.

Observe the following guidelines when installing a virtual SVP:

- vSphere Cluster Failover: Due to the numerous vSphere server/cluster configurations and workloads, validate failover prior to placing the virtual SVP in production environments.
- Number of SVP virtual machines per vSphere cluster: One server supports up to eight VMs. Each VM can communicate independently with one storage system. Due to the wide variety of vSphere server/cluster configurations and workloads, perform simultaneous multi-system performance monitoring and log collections to verify trouble-free management.

To provide the highest level of trouble-free operations, observe the following rules:

- Do not locate a virtual machine on a storage system being managed by the same virtual machine.
- Do not start the SVP virtual machine from the storage system it is managing.

Setting up the SVP locale

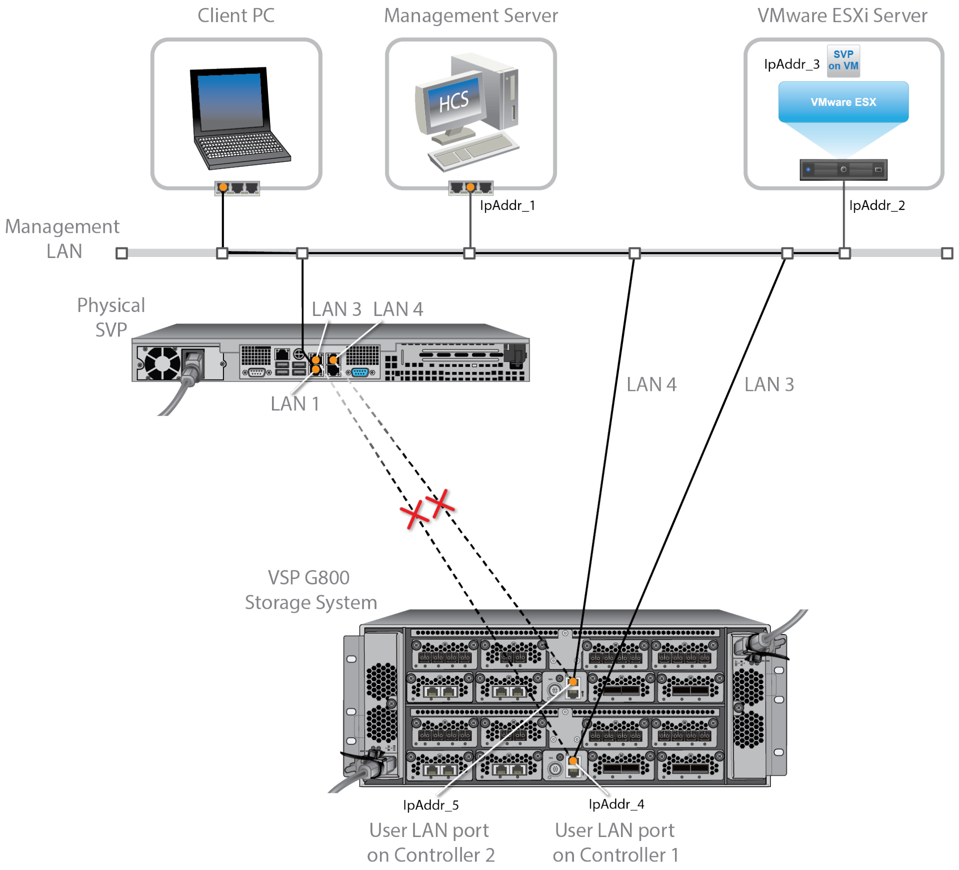
The SVP and storage management software support the English and Japanese languages.

If you intend to install the SVP software using a language other than English and Japanese, change the SVP's locale setting to reflect the appropriate language using the procedure for the Windows version installed on the SVP. For more information, see the instructions for your Windows operating system.

Network connection for virtual SVP

The SVP and storage system connection ports located at the rear of the components.

The following figure shows the physical network connection for a virtual SVP and Hitachi Virtual Storage Platform G800. Adjust your connections appropriately if using different VSP Gx00 models or VSP Fx00 models.



> **Note:** The ESXi server running the VM instance cannot be used with the storage system they belong to different subnets, and if a router or a firewall is filtering packets according to a defined condition. There is no distance limit between the server running the SVP application and the storage array being managed if they belong to the same subnet.

Virtual SVP requirements

The virtual SVP must meet the following minimum requirements.

ESX Server (provided by the customer)

- VMware ESXi server 6.x
- Two quad core processors, Intel Xeon 2.29 GHz
- One port network interface card (NIC)
- SVP guest OS
- 32 GB RAM

SVP Guest OS (maximum one DKC per SVP guest OS)

- Two virtual CPUs
- One virtual network adapter
- 4 GB RAM
- 120 GB disk space
- One of the following 64-bit operating systems:
  - For VMware ESXi 6.0.0: Windows 7 Professional (64-bit)
  - For VMware ESXi 6.0 U2: Windows 7 Professional Service Pack 1 (64-bit)

Miscellaneous

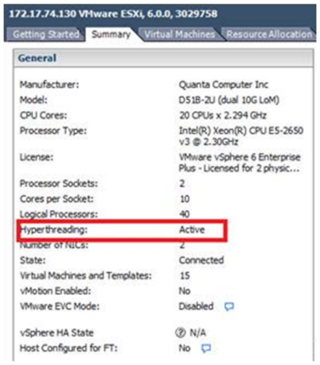
- WinZip

Hyper-threading

To support a virtual SVP, verify that hyper-threading is active for the ESXi server and VM guest host.

Note: Hyper-threading is enabled by default.

ESXi server

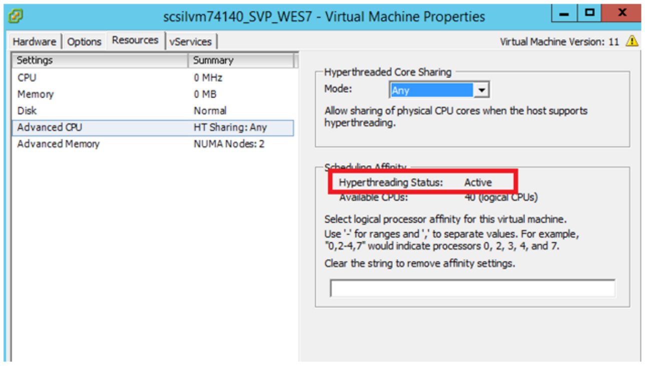


172.17.74.130 VMware ESXi, 6.0.0, 3029758

General

Manufacturer:	Quanta Computer Inc
Model:	D51B-2U (dual 10G LoM)
CPU Cores:	20 CPUs x 2.294 GHz
Processor Type:	Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz
License:	VMware vSphere 6 Enterprise Plus - Licensed for 2 physic...
Processor Sockets:	2
Cores per Socket:	10
Logical Processors:	40
Hyperthreading:	Active
Number of NICs:	2
State:	Connected
Virtual Machines and Templates:	15
vMotion Enabled:	No
VMware EVC Mode:	Disabled
vSphere HA State	N/A
Host Configured for FT:	No

VM guest host



scsilvm74140_SVP_WES7 - Virtual Machine Properties

Virtual Machine Version: 11

Settings	Summary
CPU	0 MHz
Memory	0 MB
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

Hyperthreaded Core Sharing

Mode: Any

Allow sharing of physical CPU cores when the host supports hyperthreading.

Scheduling Affinity

Hyperthreading Status: Active

Available CPUs: 40 (logical CPUs)

Select logical processor affinity for this virtual machine.

Use '-' for ranges and ',' to separate values. For example, "0,2-4,7" would indicate processors 0, 2, 3, 4, and 7.

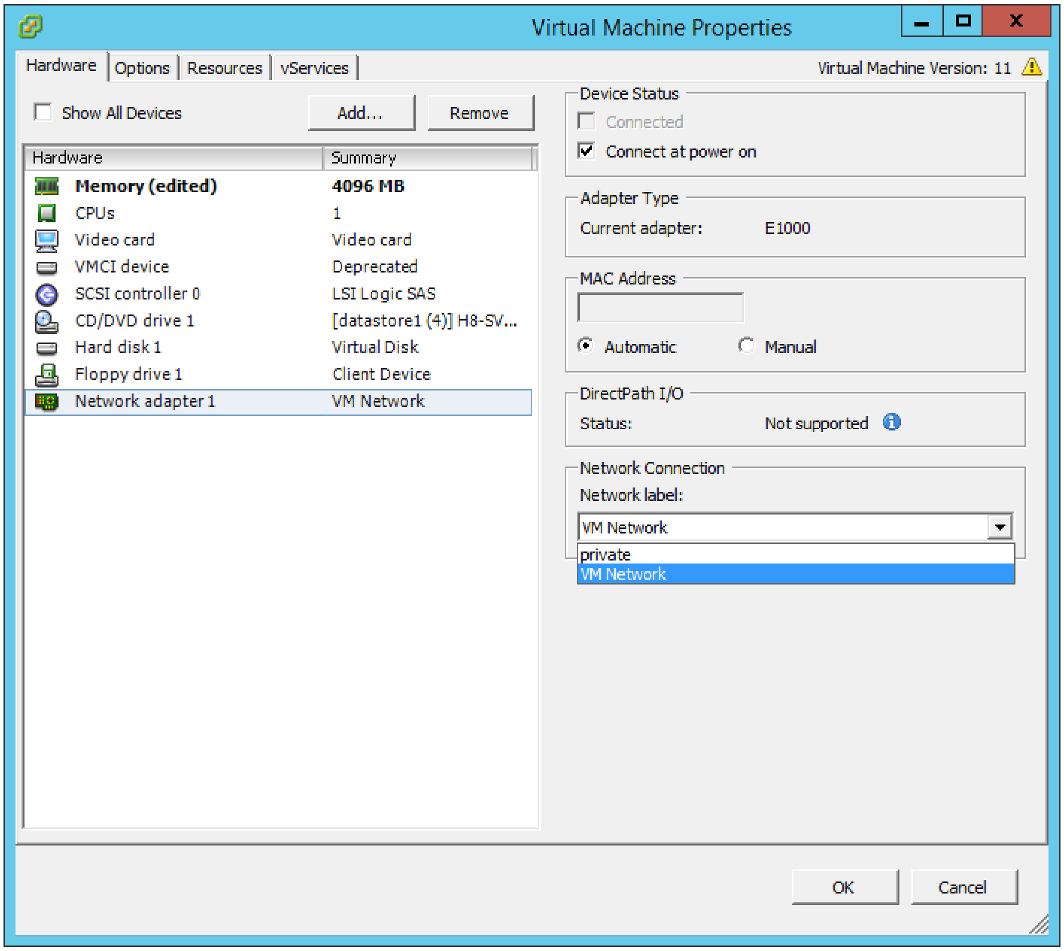
Clear the string to remove affinity settings.

Configuring the virtual SVP

After preparing the environment, activating hyper-threading on both the ESXi server and VM guest host, and verifying the configuration layout, use the following procedure to configure the virtual SVP.

Procedure

1. Create a Windows 7 Professional x64 Service Pack 1 on the ESXi host.
2. Verify the virtual network connection is properly assigned to the appropriate virtual machine network.



Virtual Machine Version: 11

□ Show All Devices

Hardware	Summary
Memory (edited)	**4096 MB**
CPUs	1
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic SAS
CD/DVD drive 1	[datastore1 (4)] H8-SV...
Hard disk 1	Virtual Disk
Floppy drive 1	Client Device
Network adapter 1	VM Network

Device Status

□ Connected

☑ Connect at power on

Adapter Type

Current adapter: E1000

MAC Address

● Automatic ○ Manual

DirectPath I/O

Status: Not supported

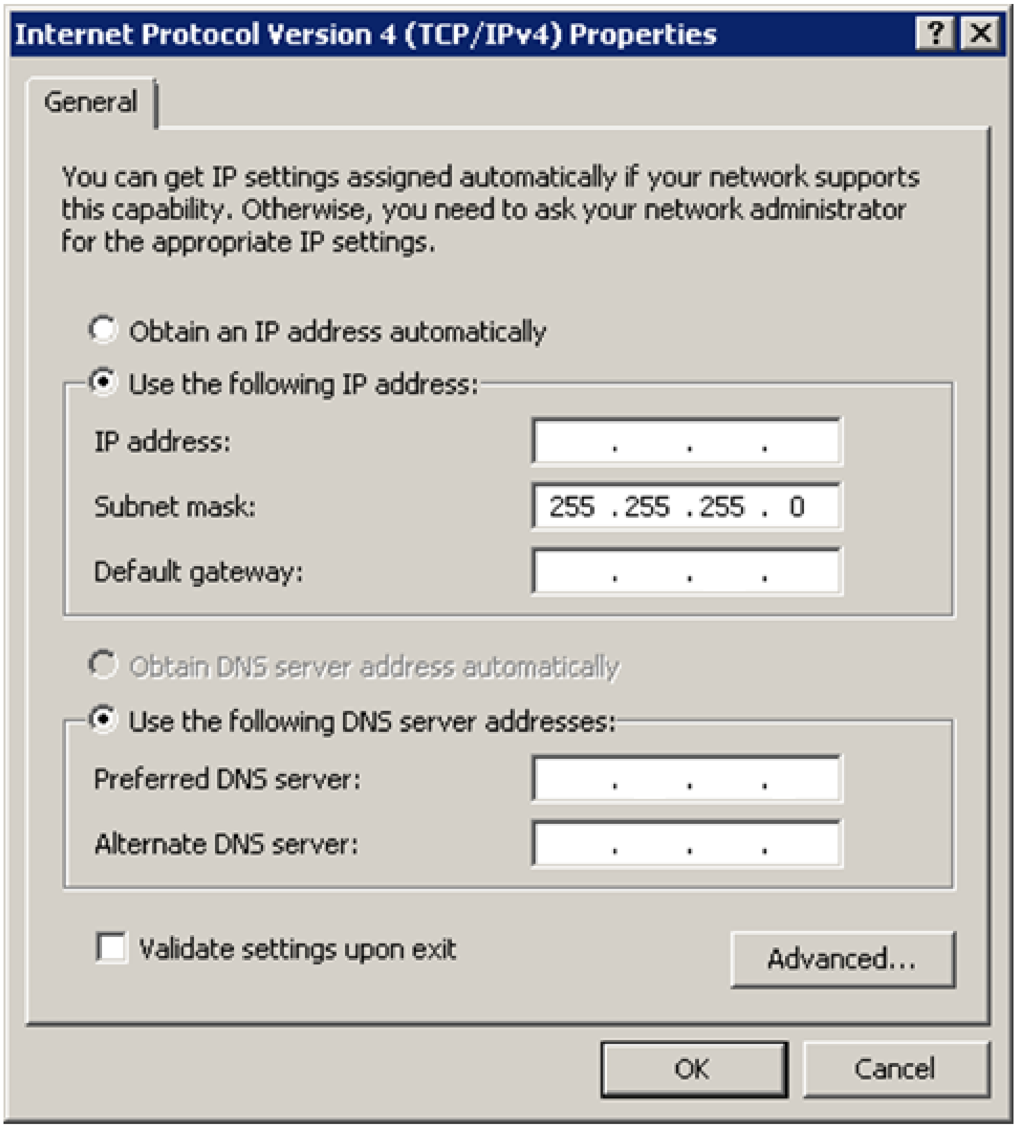
Network Connection

Network label: VM Network

private

VM Network

3. Configure network settings for the VM. The specified IP address must allow communication with the storage system controllers.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: 255 .255 .255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

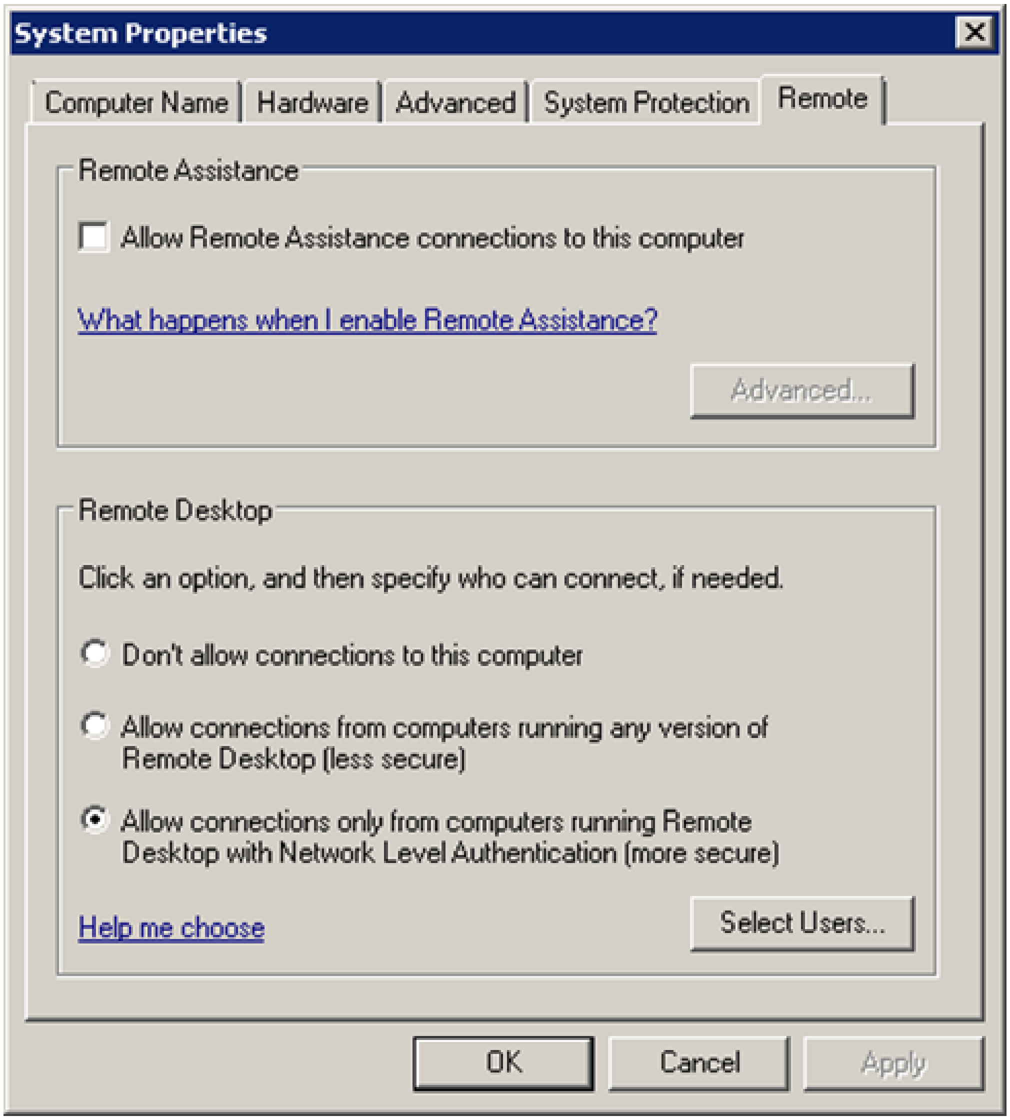
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

4. Configure a Remote Desktop connection.



Remote Assistance

□ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

● Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

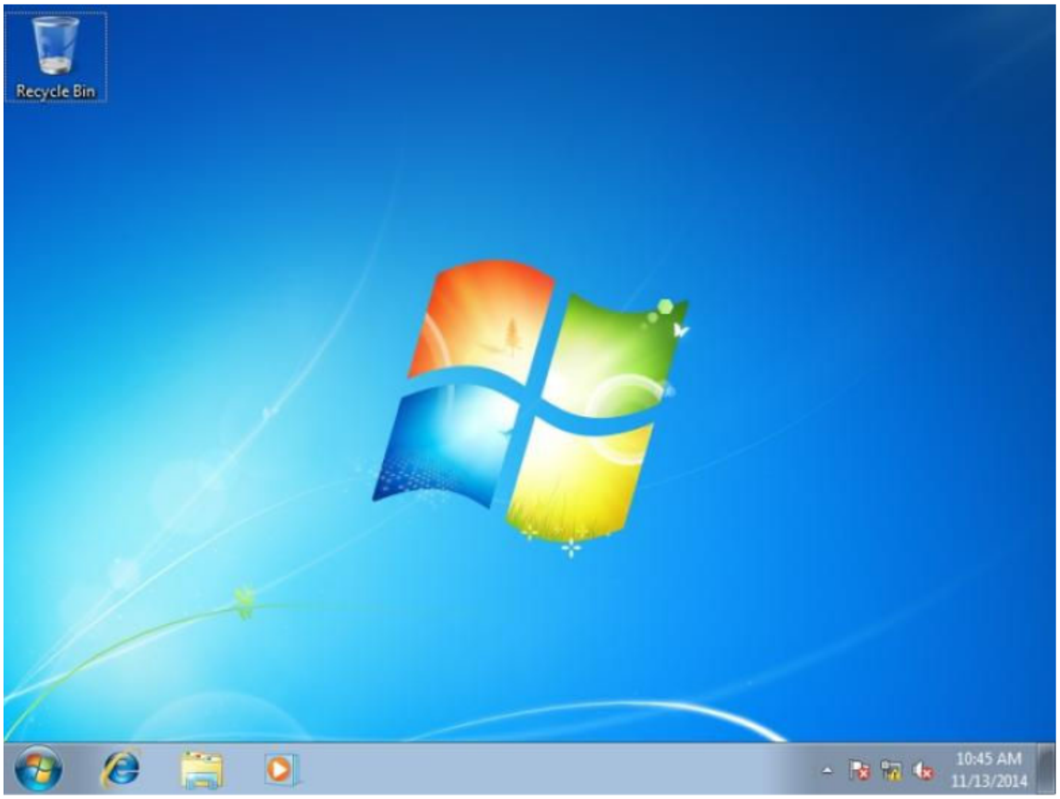
Note: After completing the configuration task, configure the SVP guest OS.

Configuring the SVP guest OS

The following procedures describe how to configure the SVP guest OS. Before you begin, ensure Hyper-Threading is active for the ESXi server and VM guest host is configured.

Logging on to the operating system

Using the Remote Desktop Connection, log on as the specified user assigned during the guest OS installation (for example, `Administrator`).



After logging on successfully, configure the control panel display.

Configuring the Control Panel display

Procedure

1. Open the Control Panel.
2. From the **View by** list, select **Large icons**.

   Note: After configuring the control panel display, configure the desktop.

Configuring the desktop

Configure the Windows screen saver function on the SVP.

Procedure

1. Click **Control Panel** > **Personalization**. For **Basic and High Contrast Themes (6)**, click **Windows Classic**.
2. Click **Screen saver**.
3. In **Screen saver**, click **Blank**, and then set **Wait** to **60 (minutes)**.
4. Click **OK**.

Next steps

Configure the task bar and the start menu properties.

Configuring the task bar and the start menu properties

Configure the Taskbar and Start menu properties on the Windows operating system running on the SVP.

Procedure

1. Click **Control Panel** > **Taskbar and Start Menu Properties (task bar property)**, and then click the **Taskbar** tab.
2. Click **Customize**.
3. In the **Notification Area Icons** window, check **Always show all icons and notifications on the taskbar**.
4. Click **OK**.
5. Click **Control Panel** > **Taskbar and Start Menu Properties (task bar property)**, and then click the **Start Menu** tab.
6. Click **Customize**.
7. In the **Customize Start Menu** window, check **Run command** and click **Display on the All Programs menu and the Start menu**.
8. Under **Music**, check **Don’t display this item**.
9. Click **OK**.
10. In the **Taskbar and Start Menu Properties** window, click **OK**.

> **Note:** After configuring the Task bar and Start Menu properties, configure the time settings.

Configuring the time settings

Configure the SVP for Universal Coordinated Time, and then configure it to not synchronize with an Internet time server.

Procedure

1. Click **Control Panel** > **Date and Time**, and then click the **Date and Time** tab.
2. Click **Change time zone**.
3. In the **Time Zone Settings** window, click **(UTC) Coordinated Universal Time**, and then click **OK**.
4. Click **Control Panel** > **Date and Time**, and then click the **Internet Time** tab.
5. Click **Change settings**. In the **Internet Time Settings** window, uncheck **Synchronize with an Internet time server**, and then click **OK**.
6. In the **Date and Time** window, click **OK**.

> **Note:** After configuring the time settings, configure the region settings.

Configuring region settings

Configure the region and language the language for your region or preference.

Procedure

1. Click **Control Panel** > **Region and Language**, and then click the **Keyboards and Languages** tab.
2. Click **Change keyboards**.
3. In the **Text Service and Input Languages** window, click the **Language Bar** tab.
4. Click **Hidden**, and then click **OK**.
5. Click **Control Panel** > **Region and Language**, and then click the **Administrative** tab.
6. Click **Change system locale**.
7. In the Region and Language settings window, for **Current system locale**, select the language for your region or preference.
8. Click **OK**.
9. In the **Change System Locale** window, click **Restart now**.
10. After the restart, click **Control Panel** > **Region and Language**, and then click the **Keyboards and Languages** tab.
11. Click **Change Keyboards**, and then click the **General** tab.
12. In the **Text Services and Input Languages** window, if **Japanese(Japan)** appears under **Installed services**, click the current selection, and then click **Remove**.
13. Click **OK**.
14. In the **Region and Language** window, click **OK**.

> **Note:** After configuring the region settings, configure the power management settings.

Configuring the power management settings

For optimum performance, the SVP requires specific power management settings.

Procedure

1. Click **Control Panel** > **Power Options**, and then click the **Show additional plans** list.
2. Click **Change settings that are currently unavailable**.
3. Click **High Performance** and **Change plan settings**.
4. In the **Edit Plan Setting** window, click **Change settings that are currently unavailable**.
5. In **Turn off the display**, select **Never**, and then click **Change advanced power settings**.
6. In the **Advanced settings** tab of the **Power Options** window, click **Change settings that are currently unavailable**. Then click **Hard disk** > **Turn off hard disk after**, and select **Never**.

7. Click **Processor power management** > **Minimum processor state**, and then select `5`.
8. Click **OK**.
9. In the **Edit Plan Setting** window, click **Save change**, and then close the window.

> **Note:** After defining the power management settings, configure the Action Center settings.

Configuring Action Center settings

All settings in the Windows Action Center must be disabled.

Procedure

1. Click **Control Panel** > **Action Center**, and then click **Change Action Center settings**.
2. In the **Change Action Center settings** window, clear all the items, click **OK**, and then close the window.

> **Note:** After configuring Action Center settings, configure the troubleshooting settings.

Configuring the troubleshooting settings

The Windows Computer Maintenance setting must be disabled.

Procedure

1. Click **Control Panel** > **Troubleshooting**, and then click **Change settings**.
2. In the **Change settings** window, for **Computer Maintenance**, click **Off**, and clear all configuration options below **Other settings**.
3. Click **OK**, and then close the window.

> **Note:** After configuring the troubleshooting settings, configure the Remote Desktop settings.

Configuring the Remote Desktop settings

Remote access to the SVP is required and appropriate Windows firewall settings must be configured.

Procedure

1. Click **Control Panel** > **System**, and then click **Remote settings**.
2. In the **System Properties** window, click the **Remote** tab.
3. Under **Remote Assistance**, clear **Allow Remote Assistance connections to this computer**.

4. Under **Remote Desktop**, click **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**.
5. Click **OK**.
6. If a message states that the Remote Desktop Firewall will be enabled, click **OK**.
7. Click **OK** to close the **System Properties** window.
8. Close the **System** window.
9. Click **Control Panel** > **Windows Firewall**, and then click **Allow a program or feature through Windows firewall**.
10. Click **Change settings**, and then verify **Remote Desktop** and **Remote Desktop - RemoteFX** for both **Home/Work (Private)** and **Public** are selected.
11. Click **OK**.
12. Close the **Windows Firewall** window.

> **Note:** After configuring the Remote Desktop settings, configure the Internet Explorer settings.

Configuring Internet Explorer settings

Configure Internet Explorer advanced, security, and properties settings.

Procedure

1. Click **Control Panel** > **Internet Options**, and then click the **Advanced** tab to modify the settings.
2. Under **Security**, select **Allow active content to run in files on My Computer**.
3. Clear **Use SSL 3.0**.
4. If **SSL 2.0** is selected, clear it.
5. Select **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2**.
6. Click **OK**.
7. Close the **Internet Properties** window.
8. From the **Control Panel** window, click **System and Security** > **Action Center**.
9. If the **SmartScreen Filter** window appears, click **OK**.
10. Click **All Programs** > **Internet Explorer**.
11. If the **Set Up Windows Internet Explorer 8** window appears, click **Next**.
12. In the **Turn on Suggested Sites** window, click **No, don’t turn on**, and then click **Next**.
13. In the **Choose your settings** window, click **Use express settings**, and then click **Finish**.
14. When an error indicates that an Internet connection is not established, close Internet Explorer.

> **Note:** After configuring Internet Explorer settings, disable the auto-execute feature.

Disabling the auto-execute feature

The SVP requires the Windows AutoPlay feature be turned off.

Procedure

1. Click **Start** > **Run**, and then type `gpedit.msc` to start the Group Policy Editor.
2. Click **Local Computer Policy** > **Computer Configuration**, click **Administrative Templates** > **Windows Components**, and then click **AutoPlay Policies**.
3. From the items on the right, double-click **Turn off Autoplay**.
4. In the **Property** window, click **Enabled** and select **All drives**, and then click **OK**.
5. Close the Group Policy Editor.
6. Click **Control Panel** > **Autoplay**.
7. Clear **Use Autoplay for all media and devices**, and then click **Save**.

   Note: After disabling the auto-execute feature, configure the Registry.

Configuring the Registry

Use Regedit to edit the Windows Registry on the SVP.

Procedure

1. Disable anonymous logon (null connection):
   a. Click **Start** > **Run**, and then type `regedit` and press **Enter**.
   b. In the **User Account Control** menu, click **Yes** to open the **Registry Editor** window.
   c. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
   d. Double-click **restrictanonymous**.
   e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.
2. Disable the beep when Remote Desktop Connection is connected:
   a. In the **Registry Editor** window, navigate to `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server`.
   b. In the **Edit** menu, click **New** > **DWORD (32-bit) Value**.
   c. Type `DisableBeep`.
   d. Double-click **DisableBeep**.
   e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.
3. Configure Remote Desktop Connection:
   a. In the **Registry Editor** window, navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services`.
   b. In the **Edit** menu, click **New** > **DWORD (32-bit) Value**.
   c. Type `fPromptForPassword`.
   d. Double-click **fPromptForPassword**.

   e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.
   f. In the **Edit** menu, click **New** > **DWORD (32-bit) Value**.
   g. Type `SecurityLayer`.

4. Restart the server.

   Note: After configuring the Registry, enable ICMP (ping) reply.

Enabling ICMP (ping) reply

The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. The protocol is used by network devices, such as routers, to send error messages and operational information indicating, as an example, a requested service is not available or a host or router could not be reached.

Procedure

1. Click **Control Panel** > **Administrative Tools**, and then start **Windows Firewall with Advanced Security**.
2. In the left pane, click **Inbound Rules**.
3. Click all the following inbound rules, and then right-click and click **Enable Rules**.
   - File and Printer Sharing (Echo Request - ICMPv4-In) (Profile=Domain)
   - File and Printer Sharing (Echo Request - ICMPv4-In) (Profile=Private)
   - File and Printer Sharing (Echo Request - ICMPv6-In) (Profile=Domain)
   - File and Printer Sharing (Echo Request - ICMPv6-In) (Profile=Private)

   Note: After enabling ICMP (ping) reply, change the computer name.

Changing the computer name

Changing the computer name allows the SVP to be identified easily.

Procedure

1. Click **Control Panel** > **System**, and then click **Change settings** under **Computer name, domain, and workgroup settings**.
2. In the **System Properties** window, click the **Computer Name** tab, and then click **Change**.
3. In the **Computer Name** field, type `SVP-PC`.
4. When prompted to restart your computer, click **OK**.
5. Click **Close**.
6. Click **Restart Now**.
7. Wait for the server to restart.

   Note: After changing the computer name, change the account name.

Changing the account name

The following user names might differ from the user name that was specified during the Windows installation.

Procedure

1. Click **Control Panel** > **User Accounts**, and then click **Change your account name**.
2. Type `SVP` for the new account name, and then click **Change Name**.
3. Close the **User Accounts** window.
4. Click **Control Panel** > **Administrative Tools**, and then click **Computer Management**.
5. Click **Computer Management (Local)** > **System Tools**, and then click **Local Users and Groups** > **Users**.
6. In the right window, right-click **User**, and then click **Rename**.
7. Rename **User** to **SVP**.
8. Close the **Computer Management** window, and then close the **Administrative Tools** window.

   Note: After changing the account name, configure the password setting for the Administrator.

Configuring the password setting for Administrator

The Windows Administrator password must be configured for use with the SVP.

Procedure

1. Click **Control Panel** > **Administrative Tools**, and then click **Computer Management**.
2. Click **Computer Management (Local)** > **System Tools**, and then click **Local Users and Groups** > **Users**.
3. In the right window, right-click **Administrator**, and then click **Set Password**.
4. In the warning message, click **Proceed**.
5. In the **New password** and **Confirm password** fields, type the administrator password `raid-login`.
6. Click **OK**.
7. Close the **Computer Management** window, and then close the **Administrative Tools** window.
8. Restart Windows.

   Note: After configuring the password setting for Administrator, change the password setting.

Changing the password setting

Change the password for the Windows operating system running on the SVP.

Procedure

1. Click **Control Panel** > **User Accounts**.
2. Click **Create a password for your account**.
3. In the top two fields, type the password `raid-login`. Leave the password hint field empty.
4. Click **Create password**.
5. Close the window.

   Note: After changing the password setting, install the SVP software.

Installing the SVP software

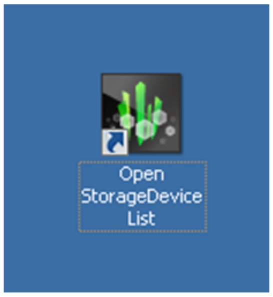
You install the SVP software from the SVP ISO image for your storage system. This image is part of the microcode distribution set and has the file name **`H8-SVP-XXX-XX.iso`**.

Procedure

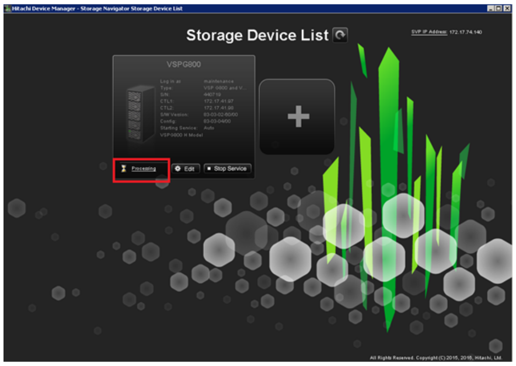
1. Obtain the appropriate SVP ISO image for your storage system from the firmware distribution set. Verify the ISO image corresponds to the firmware currently running on the storage system.
2. Download the SVP ISO from TISC to the CE notebook, and then use an ISO reader to mount the SVP ISO as the next available drive letter.
3. Launch Remote Desktop Connection and click the **Show Options** drop-down menu.
4. Click the **Local Resources** tab, and then click **More**.
5. Expand **Drives**, and then check the drive that has the ISO.
6. Click **Connect**.
7. When prompted to enter your credentials, enter your SVP password and click **OK**.
8. Perform the appropriate step:
   - If you have WinZip installed on the VM, extract the ISO locally, and then go to step 9 to run the setup application.
   - Otherwise, click the mapped drive in the left pane and double-click the **Setup** application in the workspace to the right of the pane (see the following figures), and then go to step 9.

   Note: Using WinZip is the preferred method. The alternative method performs the installation over the network and can take significantly longer to complete.
9. In the **Windows Security Alert** window, select **Private networks, such as my home or work network**. Then clear **Public networks, such as those in airports and coffee shops (not recommended because the networks often have little or no security)**.
10. Type the SVP IP address.
11. Click **Apply**.
12. Add the storage system.

13. Register the storage system.
14. Click the storage system.
    You are presented with the following two options:
    - Upgrading the firmware and adding the storage system
    - Adding the storage system without upgrading the firmware
15. If the storage system firmware is current, click **Select Update Objects** and clear **Firmware (Storage System)**. Doing so adds the storage system without upgrading the firmware.
16. Click **Apply**, and then click **Confirm** to added the storage system to the SVP.
17. On the Desktop, click the **Open StorageDevice List** shortcut.



Wait 10-15 minutes for all the services to start.



Hitachi Device Manager - Storage Navigator Storage Device List

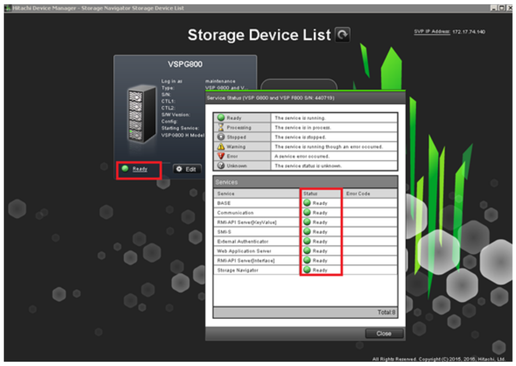
Storage Device List

SVP IP Address: 172.17.74.140

VSPG800

Log in as	maintenance
Type:	VSP G800 and V...
S/N:	440719
CTL1:	172.17.41.97
CTL2:	172.17.41.98
S/W Version:	83-03-02-60/00
Config:	83-03-04/00
Starting Service:	Auto
VSP G800 H Model	

Processing
Edit
Stop Service
+
All Rights Reserved. Copyright (C) 2015, 2016, Hitachi, Ltd.



Hitachi Device Manager - Storage Navigator Storage Device List

Storage Device List

SVP IP Address: 172.17.74.140

VSPG800

Log in as	maintenance
Type:	VSP G800 and V...
S/N:	
CTL1:	
CTL2:	
S/W Version:	
Config:	
Starting Service:	
VSP G800 H Model	

Service Status (VSP G800 and VSP F800 S/N: 440719)

Ready	The service is running.
Processing	The service is in process.
Stopped	The service is stopped.
Warning	The service is running though an error occurred.
Error	A service error occurred.
Unknown	The service status is unknown.

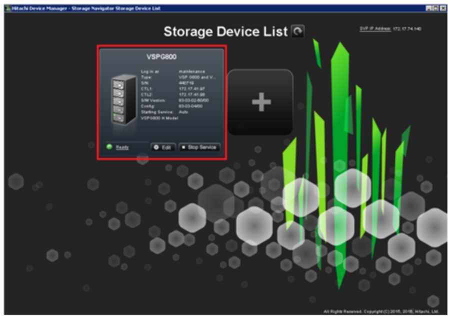
Services

Service	Status	Error Code
BASE	Ready	
Communication	Ready	
RMI-API Server[KeyValue]	Ready	
SMI-S	Ready	
External Authenticator	Ready	
Web Application Server	Ready	
RMI-API Server[Interface]	Ready	
Storage Navigator	Ready	

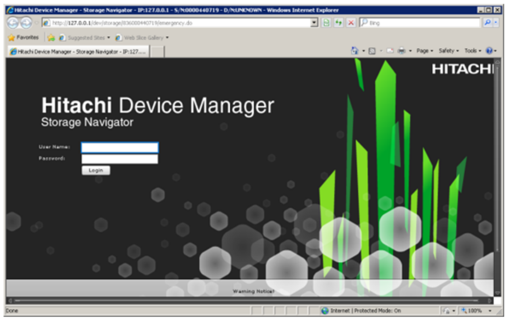
Total:8

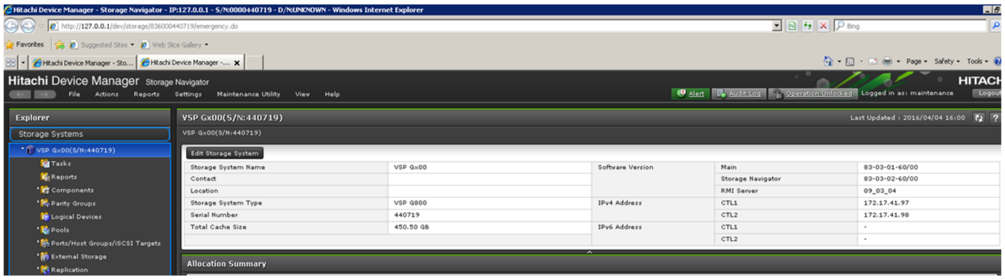
Ready
Edit
Close
All Rights Reserved. Copyright (C) 2015, 2016, Hitachi, Ltd.

18. After the services are ready, click the storage system to start Hitachi Device Manager - Storage Navigator.



Hitachi Device Manager - Storage Navigator Storage Device List





Hitachi Device Manager - Storage Navigator - IP:127.0.0.1 - S/N:0000440719 - D/N:UNKNOWN - Windows Internet Explorer

http://127.0.0.1/dev/storage/836000440719/emergency.do

VSP Gx00(S/N:440719)

Storage System Name	VSP Gx00	Software Version	Main	83-03-01-60/00
Contact			Storage Navigator	83-03-02-60/00
Location			RMI Server	09_03_04
Storage System Type	VSP G800	IPv4 Address	CTL1	172.17.41.97
Serial Number	440719		CTL2	172.17.41.98
Total Cache Size	450.50 GB	IPv6 Address	CTL1	-
			CTL2	-

Deploying a cloned virtual SVP

To avoid management outages for the working storage system, clone a virtual SVP image to an unregistered storage system.

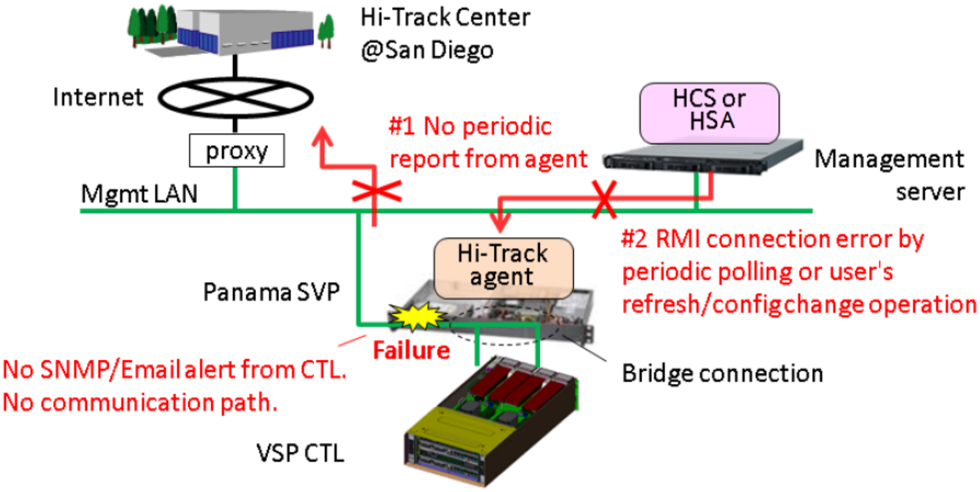
Procedure

1. Prepare a master virtual SVP image:
   a. Create the virtual SVP using the procedure in Configuring the virtual SVP (on page 66) . You do not have to set up the network at this time.
   b. Configure the SVP guest OS using the procedure in Configuring the SVP guest OS (on page 69) .
   c. Install the SVP using the procedure in Completing the configuration (on page 54) . You do not have to configure the SVP IP address at this time. In addition, do not register a DKC using the Storage Device List.
2. Turn off the master virtual SVP.
3. Clone the master virtual SVP, and then start the cloned virtual SVP.
4. Configure the Windows OS network information in the cloned virtual SVP.
5. Set the IP address for the SVP. This IP address is used to communicate with the storage system.
6. Register a storage system using the Storage Device List.

Detecting SVP failures

SVP failures are detected and resolved using the following methods.

Failure detection method	How a failure is detected	Action to be taken
Hi-Track Remote Monitoring System	No report from the agent during a 24-hour health check	Hi-Track detects SVP failure -> SVP replacement. For information about Hi-Track, go to the Hi-Track website: http://hitrack.hds.com/.
Hitachi Command Suite (HCS)	RMI connection error (not alert)	See the *Hitachi Command Suite Administrator Guide* (MK-90HC175).
Hitachi Storage Advisor (HSA)	Hardware alerts appear in Alert tiles, along with drill-down views for detailed information.	See *Hitachi Storage Advisor User Guide* (MK-94HSA004).



Chapter 8: Installing the SVP software on a Microsoft Hyper-V Server 2012 R2 Virtual Machine

You can install the SVP software on a Windows Server 2012 R2 (64-bit), Windows Server 2016 (64-bit) or Windows 10 Enterprise (64-bit) operating system running on a Microsoft Hyper-V Server 2012 R2 Virtual Machine (VM).

Setting up the SVP locale

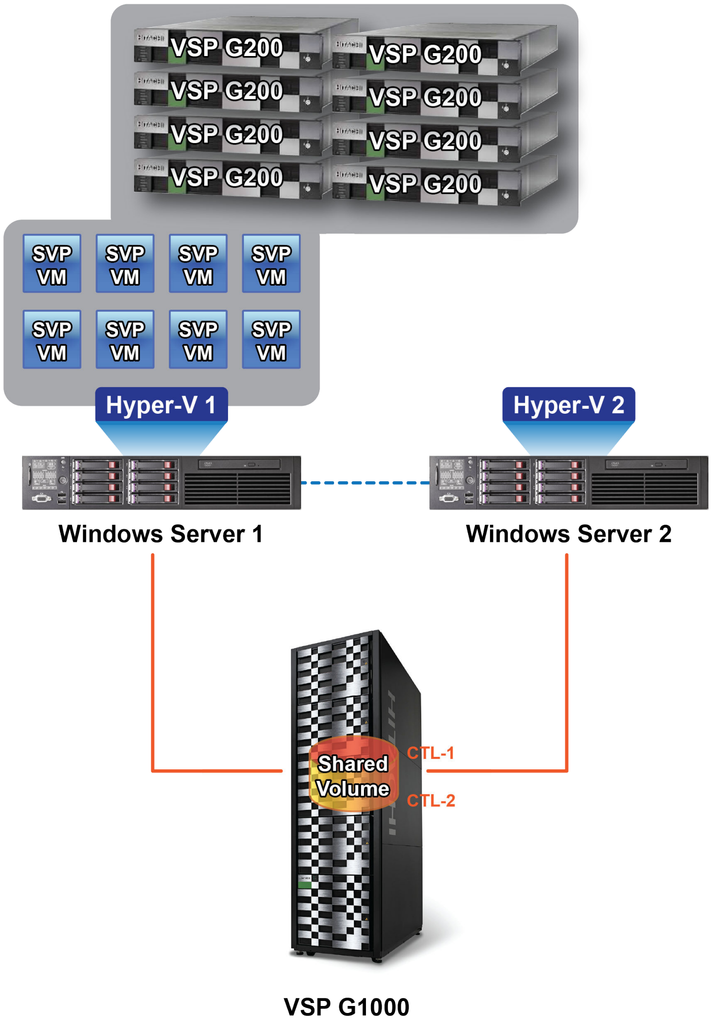
The SVP and storage management software support the English and Japanese languages.

If you intend to install the SVP software using a language other than English and Japanese, change the SVP's locale setting to reflect the appropriate language using the procedure for the Windows version installed on the SVP. For more information, see the instructions for your Windows operating system.

Network connection for Hyper-V

The following figure shows a high-level view of a Hyper-V VM implementation and migration in a non-clustered environment. In this example, eight Hitachi Virtual Storage Platform G200 storage systems are connected to a Windows server designated Hyper-V1. The Hyper-V1 server is running eight instances of SVP VMs (one for each VSP G200 storage system) and is connected to a second Windows server (Hyper-V2) that is also running Hyper-V. Both the Hyper-V1 and Hyper-V2 servers have their own connection to a Hitachi Virtual Storage Platform G1000 storage system.

Note: The Hyper-V server running the VM instance cannot be used with the storage system if it belongs to different subnets, and if a router or a firewall is filtering packets according to a defined condition. There is no distance limit between the server running the SVP application and the storage array being managed if they belong to the same subnet.



Minimum requirements for Hyper-V Server 2012 R2 VM

A host that runs the SVP software on a customer-supplied Microsoft Hyper-V Server 2012 R2 VM requires the following minimum requirements.

- Hyper-V Server Windows 2012R supplied by the customer
- Two quad core processors, Intel Xeon 2.29 GHz
- One-port NIC
- SVP guest OS
- 32-GB RAM

The SVP guest (1 DKC) (maximum one DKC per SVP guest OS)

- Two vCPUs
- One virtual network adapter
- 4-GB RAM
- 120-GB disk space
- One of the following 64-bit operating systems:
  - Windows 10 Professional
  - Windows 10 Enterprise
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016

To use Hyper-V Manager successfully, you must first configure your hosts correctly. In particular, confirm that each host:

- Is licensed for Windows 2012R2 OS.
- Meets the shared storage requirements for Hyper-V Management.
- Meets the networking requirements for Hyper-V Management.

Installing and Configuring Hyper-V on Windows 2012 R2 Server

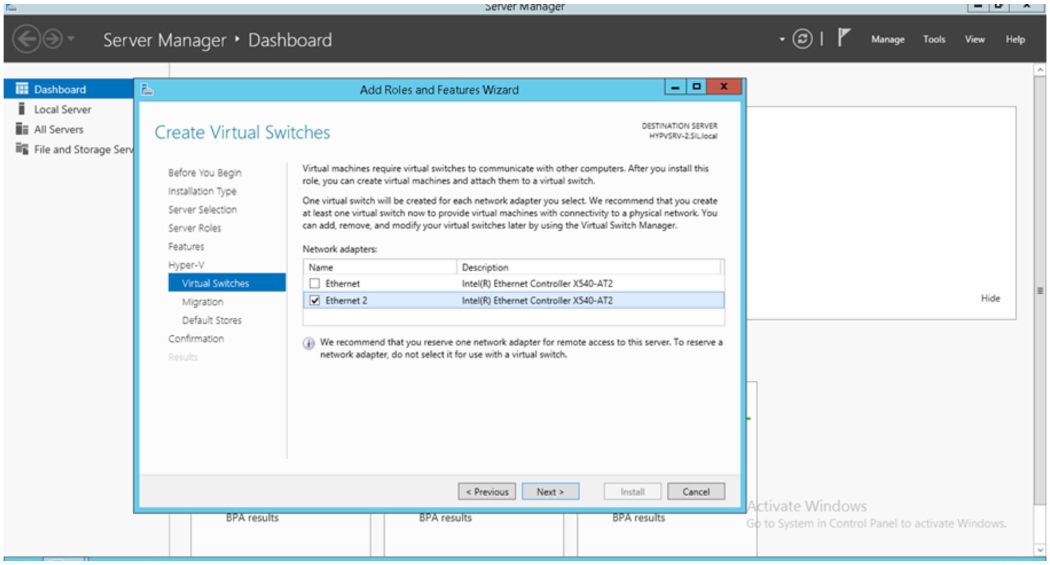
When you install and configure a customer-supplied version of Microsoft Hyper-V on Windows 2012 R2 Server, you configure the virtual switch. A virtual switch allows VMs created on Hyper-V hosts to communicate with other computers. You can also configure the default stores. Default stores are default locations for storing virtual hard disk files and virtual configuration files.

In the following procedure, you will define virtual switch settings. However, you will accept the default settings for the default stores; you can specify different locations later by modifying the Hyper-V settings.

Procedure

1. Go to **Start** > **Programs**, and then click **Administrative Tools** > **Server Manager**.
2. In the Dashboard, click **Add roles and features**.

3. In the left pane of the **Add Roles and Features Wizard** window, click **Hyper-V** > **Virtual Switches**. Then check the appropriate Ethernet controller.



Create Virtual Switches

DESTINATION SERVER
HYPVSRV-2.SIL.local

Virtual machines require virtual switches to communicate with other computers. After you install this role, you can create virtual machines and attach them to a virtual switch.

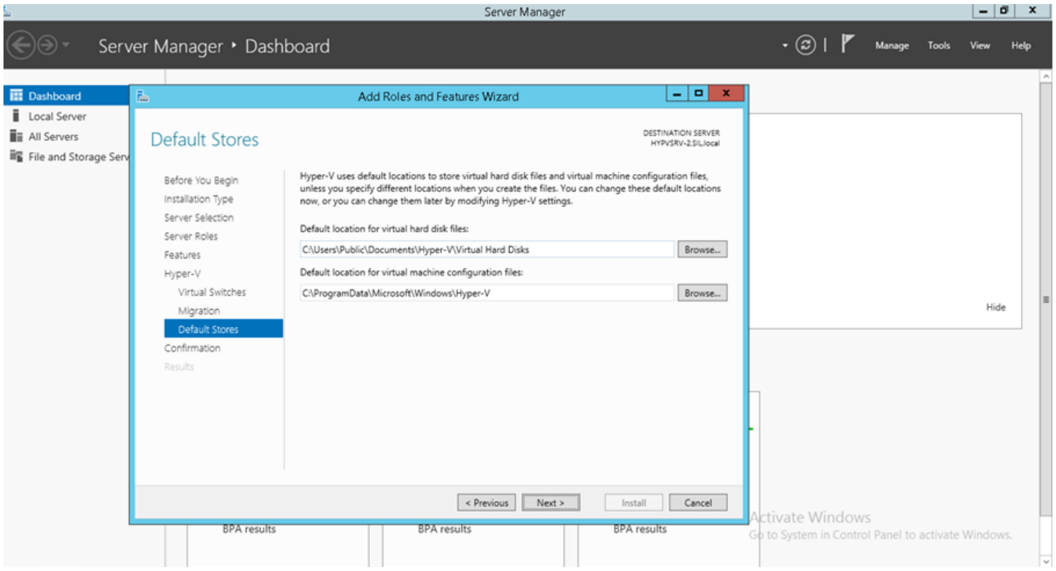
One virtual switch will be created for each network adapter you select. We recommend that you create at least one virtual switch now to provide virtual machines with connectivity to a physical network. You can add, remove, and modify your virtual switches later by using the Virtual Switch Manager.

Network adapters:

Name	Description
□ Ethernet	Intel(R) Ethernet Controller X540-AT2
☑ Ethernet 2	Intel(R) Ethernet Controller X540-AT2

We recommend that you reserve one network adapter for remote access to this server. To reserve a network adapter, do not select it for use with a virtual switch.

4. Accept the default **Hyper-V** > **Default Stores** locations for storing files. If you need to change the locations later, do so by using the Hyper-V settings.



Default Stores

DESTINATION SERVER
HYPVSRV-2.SIL.local

Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.

Default location for virtual hard disk files:
C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

Default location for virtual machine configuration files:
C:\ProgramData\Microsoft\Windows\Hyper-V

Installing the SVP software on a guest OS

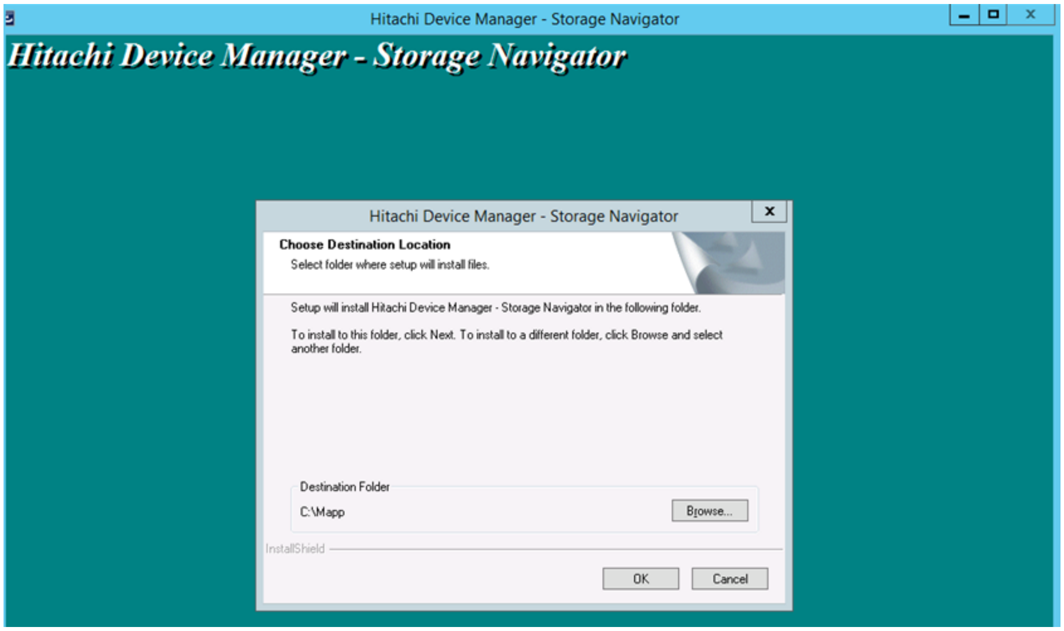
After you perform the host configuration, install the SVP software on a guest OS.

You install the SVP software using Hitachi Device Manager - Storage Navigator.

Procedure

1. Double-click the `Setup.exe` file for Device Manager - Storage Navigator.
2. When prompted, select a language and accept the license agreement.

3. Accept the default directory or select a different one, and then click **OK**.



Hitachi Device Manager - Storage Navigator
Hitachi Device Manager - Storage Navigator
Hitachi Device Manager - Storage Navigator
InstallShield
Browse...
OK
Cancel

Choose Destination Location

Select folder where setup will install files.

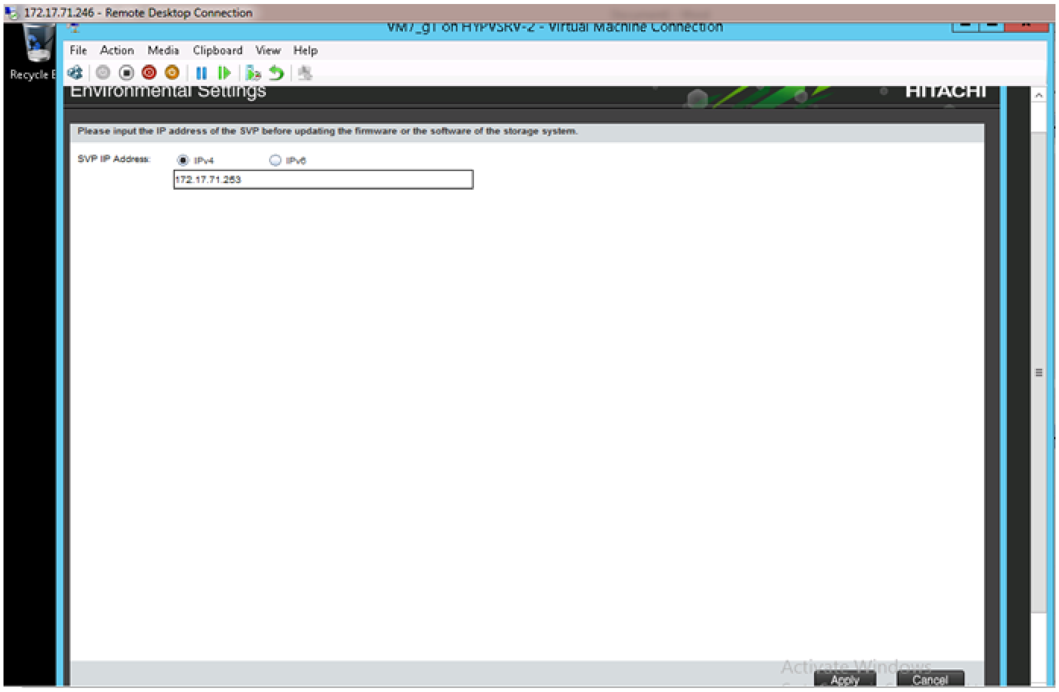
Setup will install Hitachi Device Manager - Storage Navigator in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Mapp

4. Select the IP addressing method (IPv4 or IPv5), enter the IP address of the SVP port connecting the SVP and the storage system, and then click **Apply**.

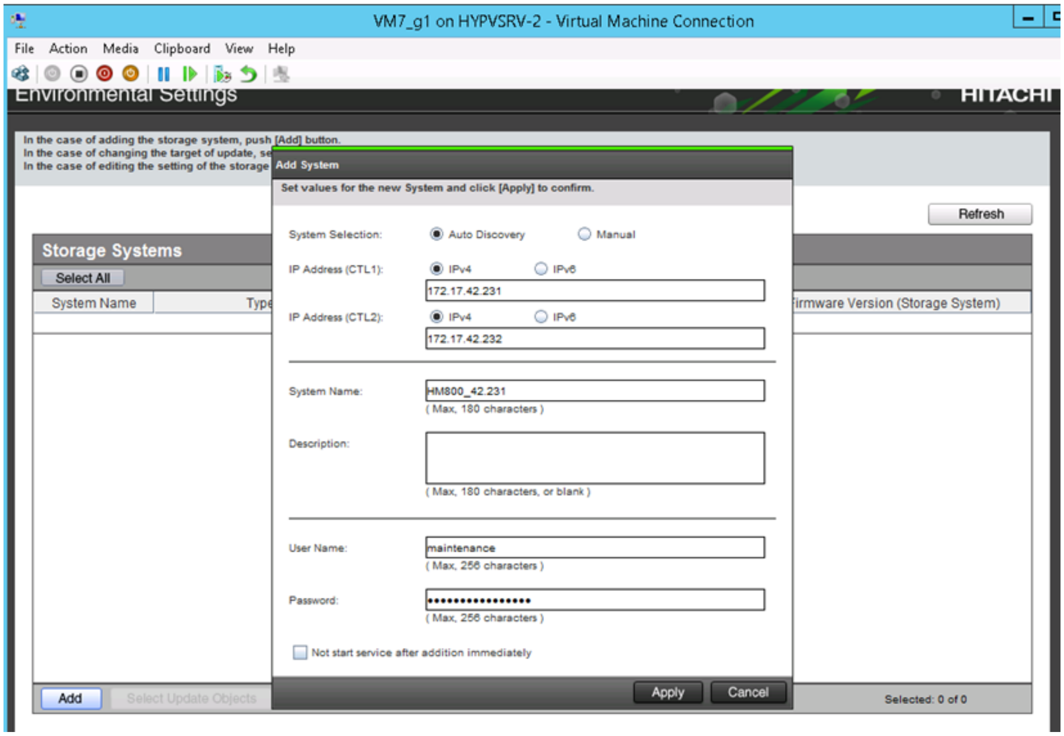


Please input the IP address of the SVP before updating the firmware or the software of the storage system.

SVP IP Address: ● IPv4 ○ IPv6

172.17.71.253

5. Complete the fields in the **Add System** window.



In the case of adding the storage system, push [Add] button.
In the case of changing the target of update, se
In the case of editing the setting of the storage

Set values for the new System and click [Apply] to confirm.

System Selection: ● Auto Discovery ○ Manual

IP Address (CTL1): ● IPv4 ○ IPv6
172.17.42.231

IP Address (CTL2): ● IPv4 ○ IPv6
172.17.42.232

System Name: HM800_42.231
(Max, 180 characters)

Description:
(Max, 180 characters, or blank)

User Name: maintenance
(Max, 256 characters)

Password: ••••••••••••••••
(Max, 256 characters)

□ Not start service after addition immediately

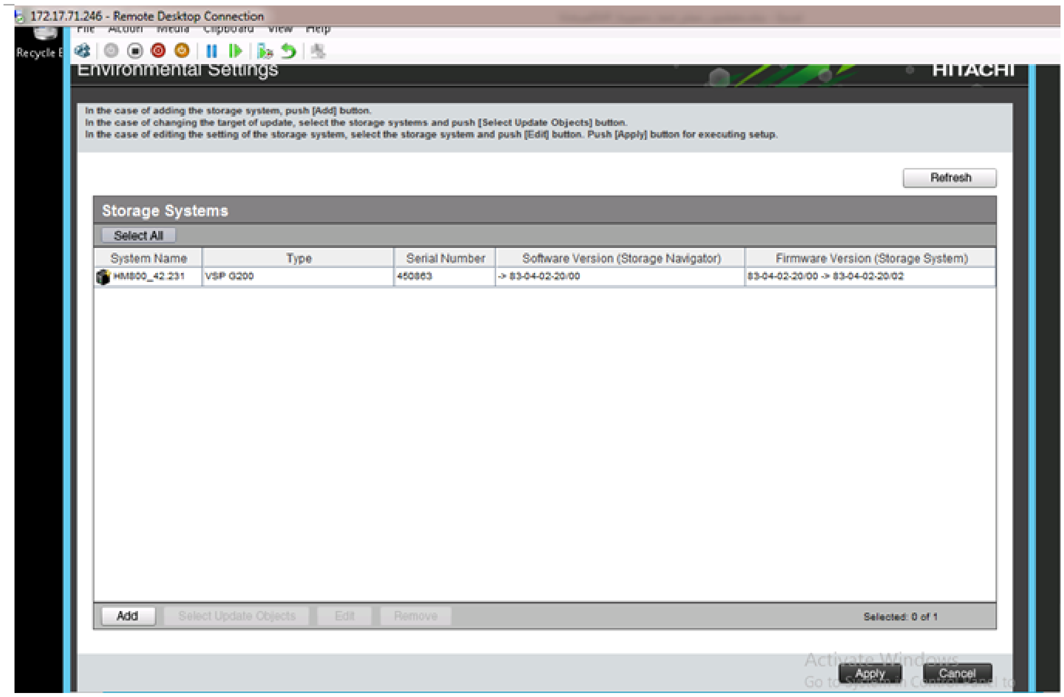
Field	Description
System Selection	Select one of the following methods to discover the storage system. ▪ Auto Discovery: Acquire the storage system information automatically. (default) ▪ Manual: Specify the storage system manually.
IP Address (CTL 1)	Enter the IP address for controller 1. Accept the default **IPv4** setting or select **IPv6**, and then enter the IP address in the appropriate format for the addressing method selected.
IP Address (CTL 2)	Enter the IP address for controller 2. Accept the default **IPv4** setting or select **IPv6**, and then enter the IP address in the appropriate format for the addressing method selected.

Field	Description
System Name	Enter the display name of the storage system, up to 180 characters. Permitted characters are one-byte alphanumeric characters and symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~). You cannot use one-byte spaces.
Description	Enter the description of the storage system, up to 360 characters.
User Name	Enter a user name. Permitted characters are one-byte alphanumeric characters and symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~).
Password	Enter a password.
Not start service after addition immediately[2]	Check if you do not want to start service after adding the storage system. (Default is unchecked.)

[1] Service personnel set the storage system information manually. User should not select **Manual** to set it.

[2] To register multiple storage systems, best practice is to check this check box for the settings so that they do not start services while they are added.

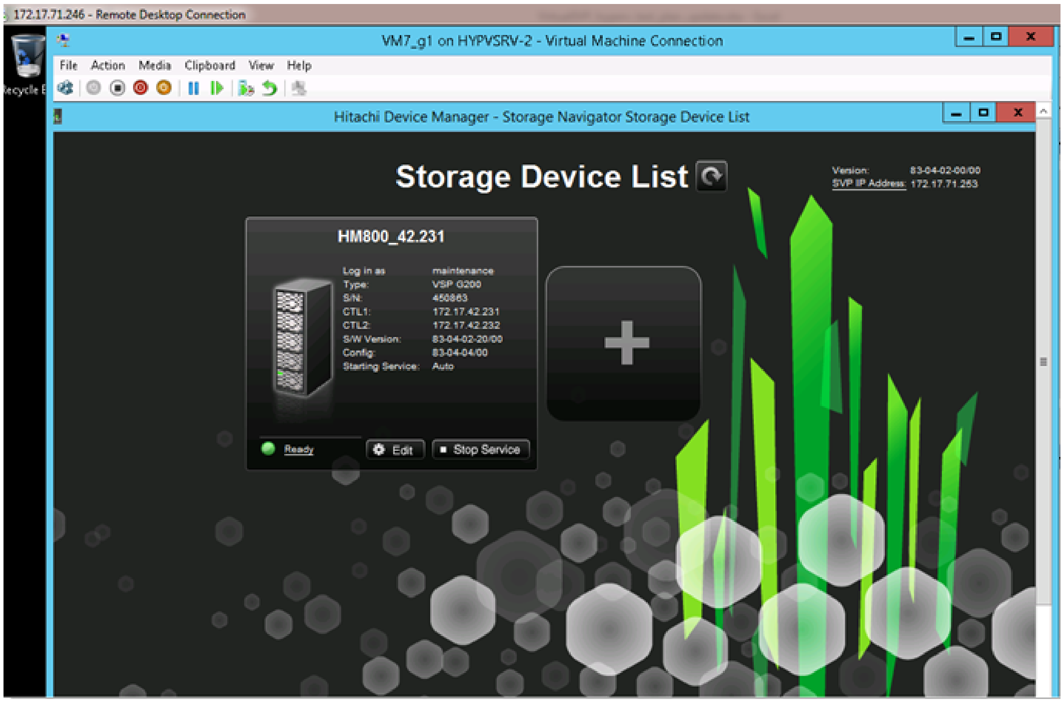
6. When the target storage systems list window opens, click **Apply**.



In the case of adding the storage system, push [Add] button.
In the case of changing the target of update, select the storage systems and push [Select Update Objects] button.
In the case of editing the setting of the storage system, select the storage system and push [Edit] button. Push [Apply] button for executing setup.

System Name	Type	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
HM800_42.231	VSP G200	450863	-> 83-04-02-20/00	83-04-02-20/00 -> 83-04-02-20/02

7. Confirm that the storage system appears in the Storage Device List.



172.17.71.246 - Remote Desktop Connection
Recycle B
VM7_g1 on HYPVSRV-2 - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Hitachi Device Manager - Storage Navigator Storage Device List
Storage Device List

Version: 83-04-02-00/00
SVP IP Address: 172.17.71.253

HM800_42.231

Log in as maintenance
Type: VSP G200
S/N: 450863
CTL1: 172.17.42.231
CTL2: 172.17.42.232
S/W Version: 83-04-02-20/00
Config: 83-04-04/00
Starting Service: Auto

Ready
Edit
Stop Service
+

This completes the procedure for installing the SVP software on a guest OS. If you need to modify your configuration, refer to the instructions for installing the SVP on a VMware ESXi host.

Chapter 9: Upgrading the SVP software

The following instructions describe how to upgrade the SVP software. Procedures are provided for upgrading the SVP software only, or installing the SVP software, Device Manager - Storage Navigator, and storage system firmware at the same time.

Important: The Hitachi Vantara-supplied SVP can only be installed, upgraded, or replaced by a Hitachi Vantara representative or an authorized service provider. Contact a Hitachi Vantara representative for more information about installing, upgrading, or replacing a Hitachi Vantara-supplied SVP.

Note: Before upgrading the SVP software:

- Back up your SVP configuration. For details about backing up your SVP configuration, see Backing up the SVP configuration (on page 163) .
- Disable the Hi-Track Remote Monitoring System. Otherwise, the upgrade procedure fails. You can enable Hi-Track after you upgrade the SVP software using Storage Device List.
- View all active alerts (see https://support.hitachivantara.com/en_us/contact-us.html).

Stopping the service in each storage system

You must stop the service to upgrade the SVP software. After the software is upgraded, you can restart the service.

In the following cases, all the storage systems with **Ready** service status must be stopped in the Storage Device List.

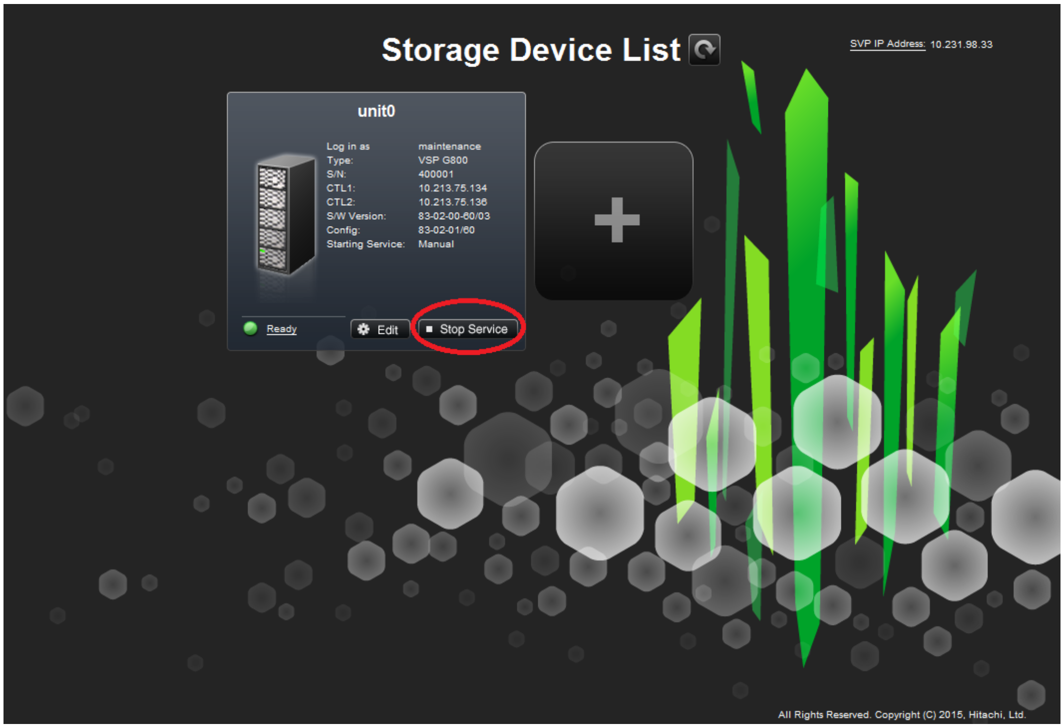
- Update the SVP software.
- Start services on storage systems running **S/W Version** 83-01-xx or later.

To stop the service, perform the following procedure from the PC connected to the SVP.

Note: When the storage system with **S/W Version** 83-01-xx or later is registered, set all the registered storage systems so that they do not start services automatically when restarting the SVP. For more information, see Changing storage system information in the Storage Device List (on page 125) .

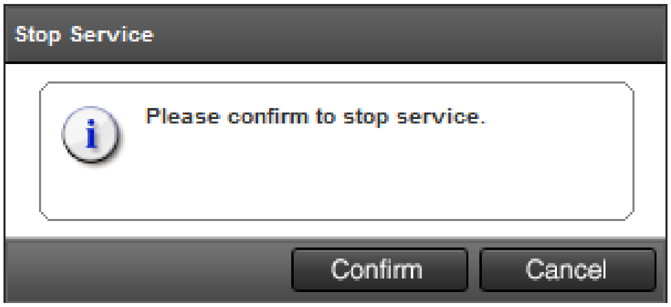
Procedure

1. In the **Storage Device List** window, click **Stop Service** of the storage system where you want to stop the service.


Storage Device List
SVP IP Address: 10.231.98.33
unit0
Ready
Edit
Stop Service
All Rights Reserved. Copyright (C) 2015, Hitachi, Ltd.

Log in as maintenance
Type: VSP G800
S/N: 400001
CTL1: 10.213.75.134
CTL2: 10.213.75.136
S/W Version: 83-02-00-60/03
Config: 83-02-01/60
Starting Service: Manual

The **Stop Service** screen opens.



Please confirm to stop service.

2. Click **Confirm**.

Note: To resume service, in the **Storage Device List** window, click **Start Service** of the storage system where you want to start the service.

Upgrading the SVP software only

This procedure describes how to upgrade the SVP software, without upgrading the storage management software and storage system firmware. This procedure can be used with storage systems that have firmware version 83-01-21 or later.

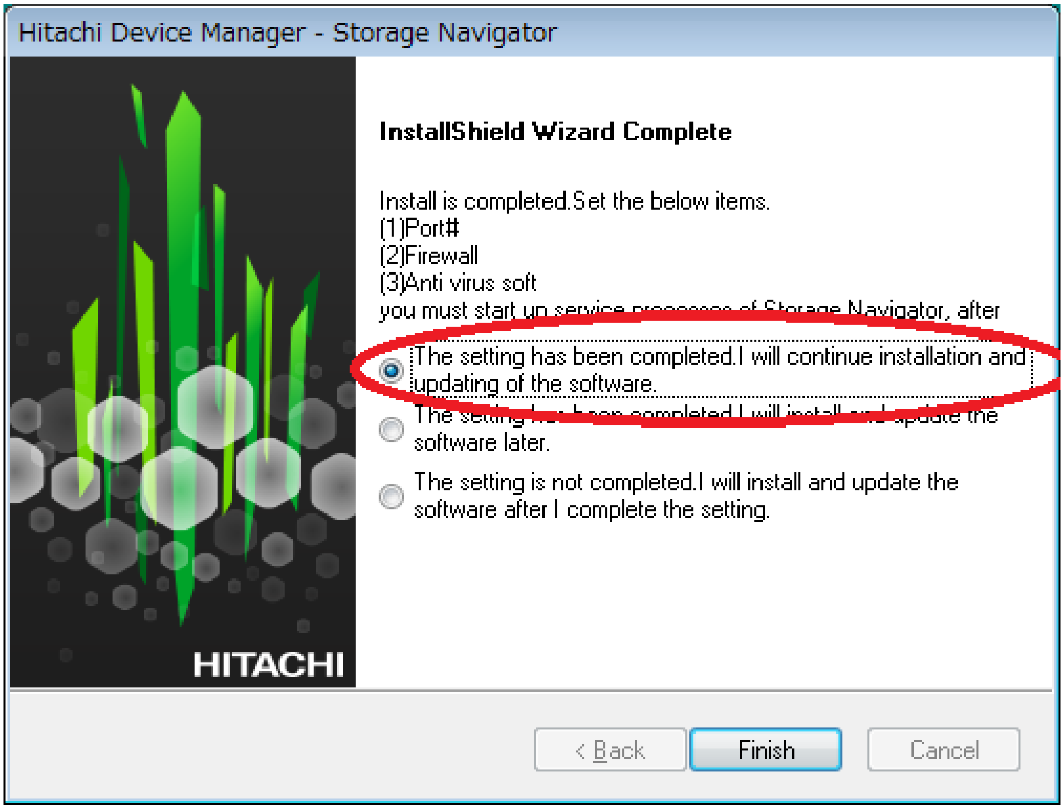
This procedure assumes that the storage system is operating and that a console PC is connected to the SVP using Remote Desktop Client.

Note: Before upgrading the SVP software:

- Disable the Hi-Track Remote Monitoring System (see http://hitrack.hds.com); otherwise, the upgrade procedure will fail. You can enable Hi-Track after you upgrade the SVP software.
- View all active alerts (see https://support.hitachivantara.com/en_us/contact-us.html).

Procedure

1. At the console PC connected to the physical SVP or running the SVP software, insert the SVP software media.
2. On the SVP, create a new folder, and then copy all of the files from the SVP software media into the new folder.
3. In the new folder, right-click the `Setup.exe` file and click **Execute as Administrator**.
4. In the following screens, click **Next**, accept the license agreement, and click **Next**, and then click **Yes**. If the **Windows Security Alert** window opens, click **Allow access**. In the following screen, click the top option, as shown, and then click **Finish**.



Hitachi Device Manager - Storage Navigator

InstallShield Wizard Complete

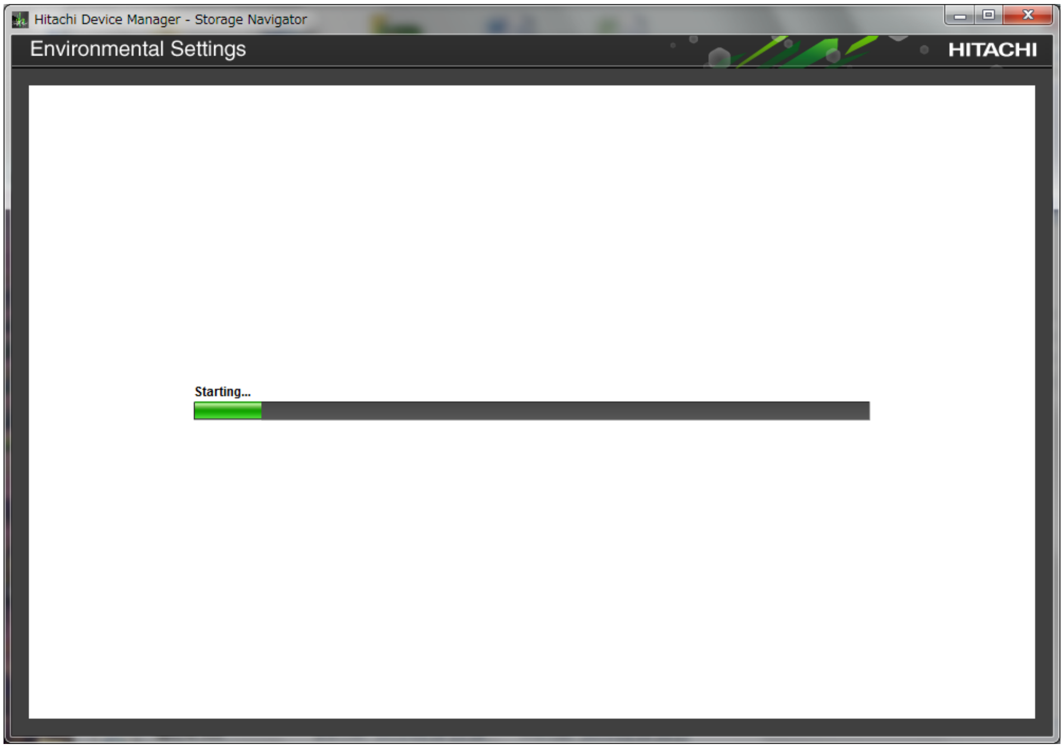
Install is completed.Set the below items.
(1)Port#
(2)Firewall
(3)Anti virus soft
you must start up service processes of Storage Navigator, after

● The setting has been completed.I will continue installation and updating of the software.

○ The setting has been completed.I will install and update the software later.

○ The setting is not completed.I will install and update the software after I complete the setting.

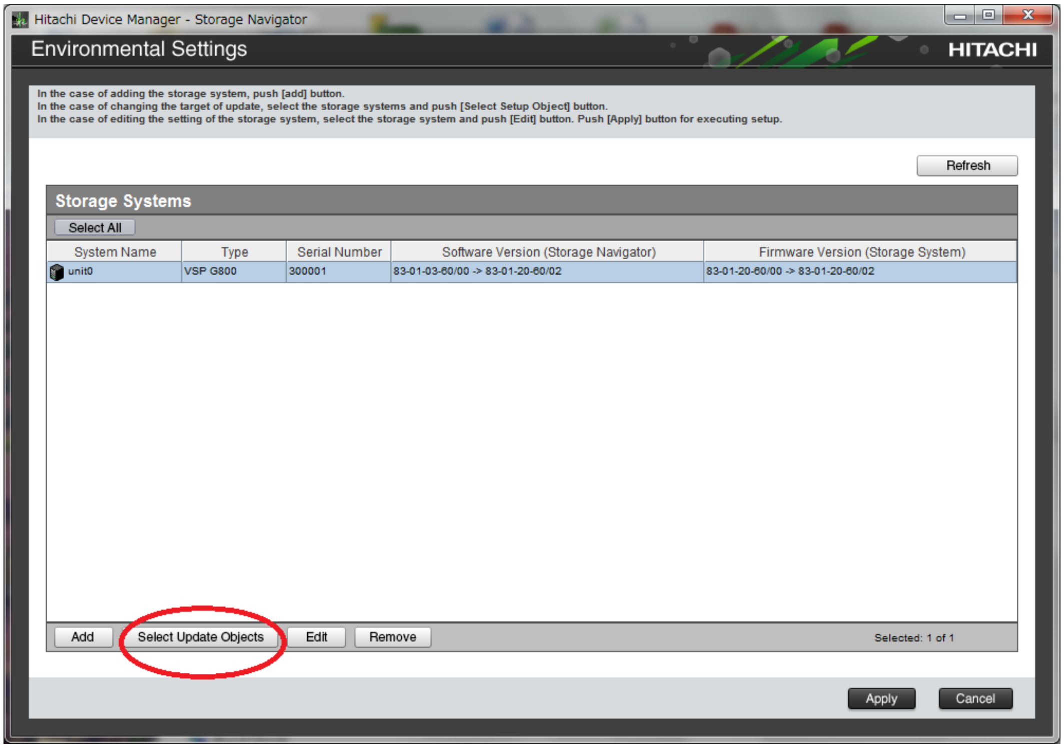
The **Environmental Settings** window opens as the system prepares for the upgrade.



Starting...

5. Wait for the preparation to complete and for the target storage systems list window to open.

6. When the target storage systems list window opens, select the appropriate storage systems, and then click **Select Update Objects**.



In the case of adding the storage system, push [add] button.
In the case of changing the target of update, select the storage systems and push [Select Setup Object] button.
In the case of editing the setting of the storage system, select the storage system and push [Edit] button. Push [Apply] button for executing setup.

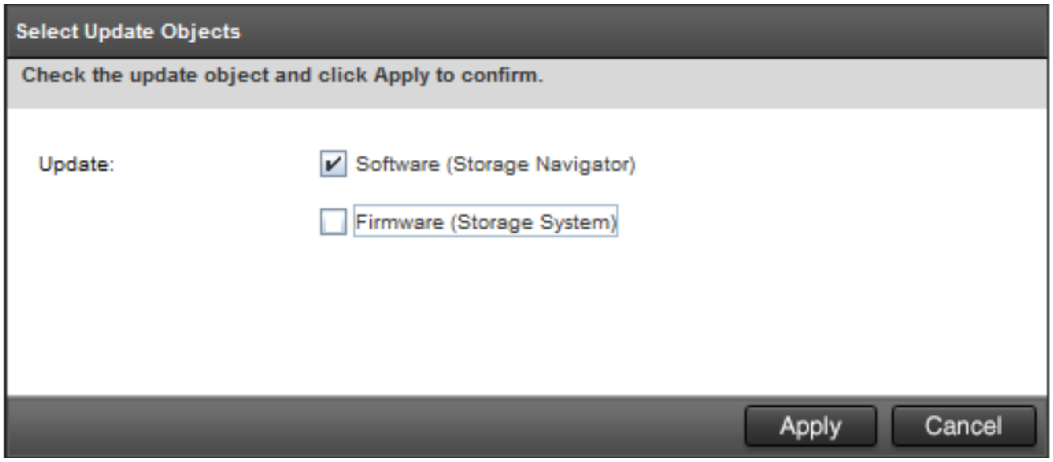
Storage Systems

System Name	Type	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
unit0	VSP G800	300001	83-01-03-60/00 -> 83-01-20-60/02	83-01-20-60/00 -> 83-01-20-60/02

Selected: 1 of 1

The **Select Update Objects** window opens.

7. Check **Software (Storage Navigator)** and uncheck **Firmware (Storage Navigator)**.



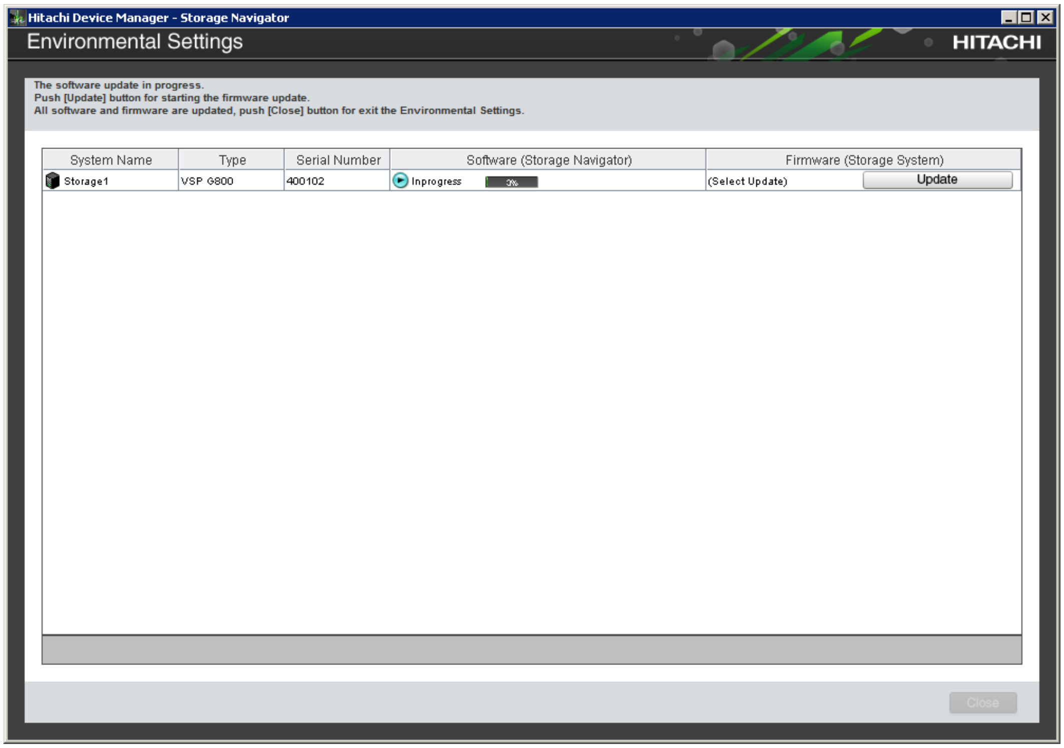
Select Update Objects

Check the update object and click Apply to confirm.

Update: ☑ Software (Storage Navigator)

□ Firmware (Storage System)

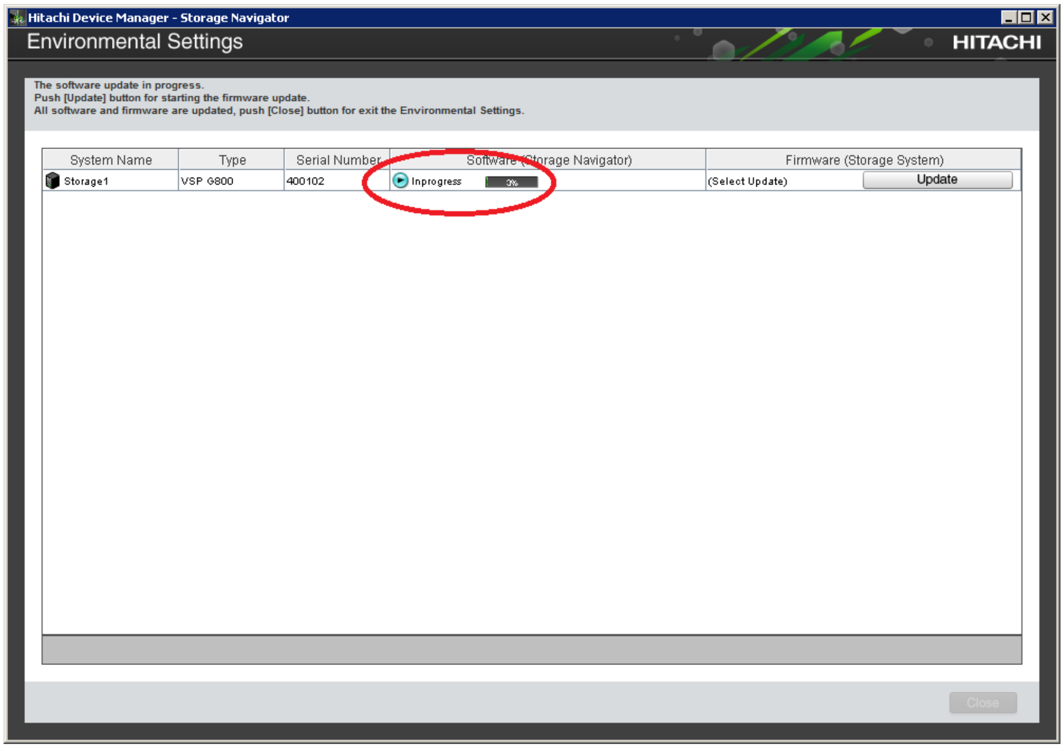
8. Click **Apply**.
   The **Update software and firmware** window opens.
9. Click **Confirm**.
   The **Run update** window opens and the software update starts automatically.



The software update in progress.
Push [Update] button for starting the firmware update.
All software and firmware are updated, push [Close] button for exit the Environmental Settings.

System Name	Type	Serial Number	Software (Storage Navigator)	Firmware (Storage System)
Storage1	VSP G800	400102	Inprogress 3%	(Select Update) Update

10. Check the upgrade status in the **Software (Storage Navigator)** row.



The software update in progress.
Push [Update] button for starting the firmware update.
All software and firmware are updated, push [Close] button for exit the Environmental Settings.

System Name	Type	Serial Number	Software (Storage Navigator)	Firmware (Storage System)
Storage1	VSP G800	400102	Inprogress 0%	(Select Update) Update

The following table shows the possible status conditions:

Status	**Description**
Waiting	Software waiting to be upgraded. Software components are upgraded individually.
In Progress	Software is running.
Completed	Software upgrade is complete.
Failed	Software upgrade failed. Click **Update** to display the **Update Firmware** window and review the error details.
(Not Update)	Not selected as a firmware upgrade target.

11. In the **Environmental Settings** window, click **Close**.
12. In the **Confirm exit** window, click **Confirm**.
13. If you disabled the Hi-Track Remote Monitoring System, enable it (see http://hitrack.hds.com).

Upgrading the storage management, SVP software, and storage system firmware

The following procedure describes how to upgrade the SVP software, Device Manager - Storage Navigator, and storage system firmware.

Before you begin

This procedure assumes the storage system is operating and a console PC is connected to the SVP through Remote Desktop Client.

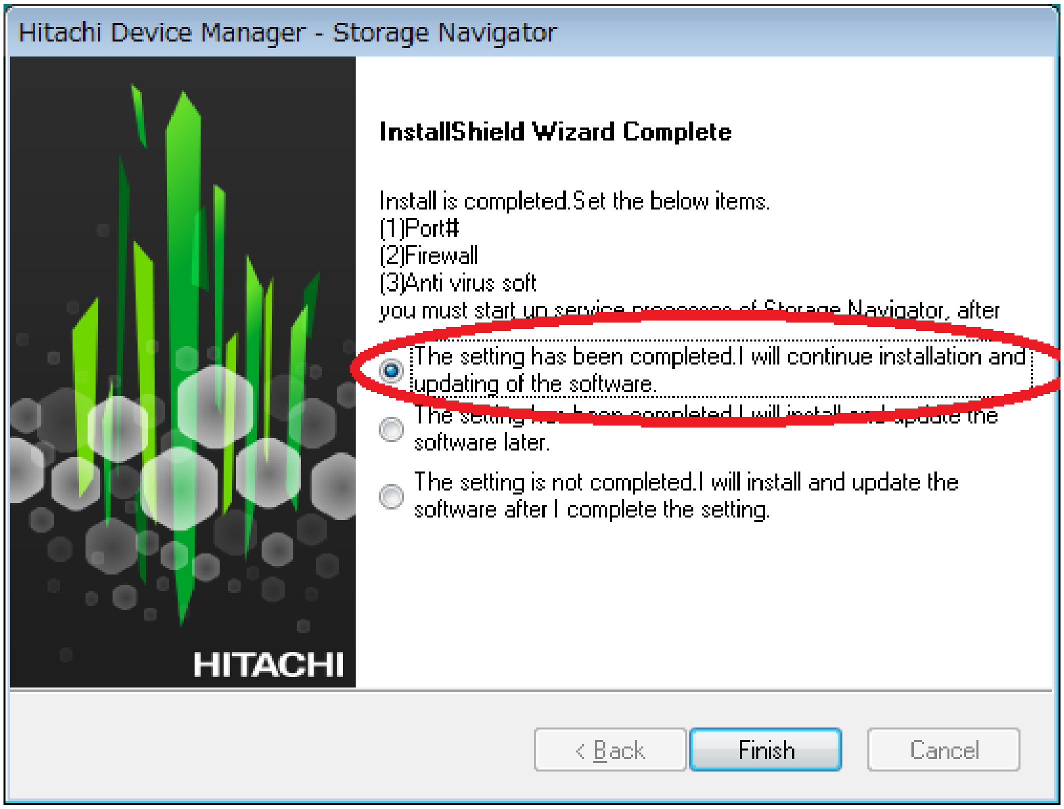
- Disable the Hi-Track Remote Monitoring System otherwise, the upgrade procedure fails. Enable Hi-Track after the SVP software upgrade is complete.
- View all active alerts (see https://support.hitachivantara.com/en_us/contact-us.html).

Note: This upgrade time is approximately 3.5 hours for storage systems with firmware version 83-01-21 or later.

Note: The upgrade time can take up to 9 hours to complete when NAS modules are installed.

Procedure

1. On the console PC connected to the physical SVP or running the SVP software, insert the SVP software media.
2. On the SVP, create a new folder, and then copy all the files from the SVP software media into the new folder.
3. In the new folder, right-click the `Setup.exe` file, and click **Execute as Administrator**.
4. In the following screens, click **Next**, accept the license agreement, and click **Next**, and then click **Yes**. If the **Windows Security Alert** window opens, click **Allow access**. In the following screen, click the top option and then click **Finish**.



Hitachi Device Manager - Storage Navigator

InstallShield Wizard Complete

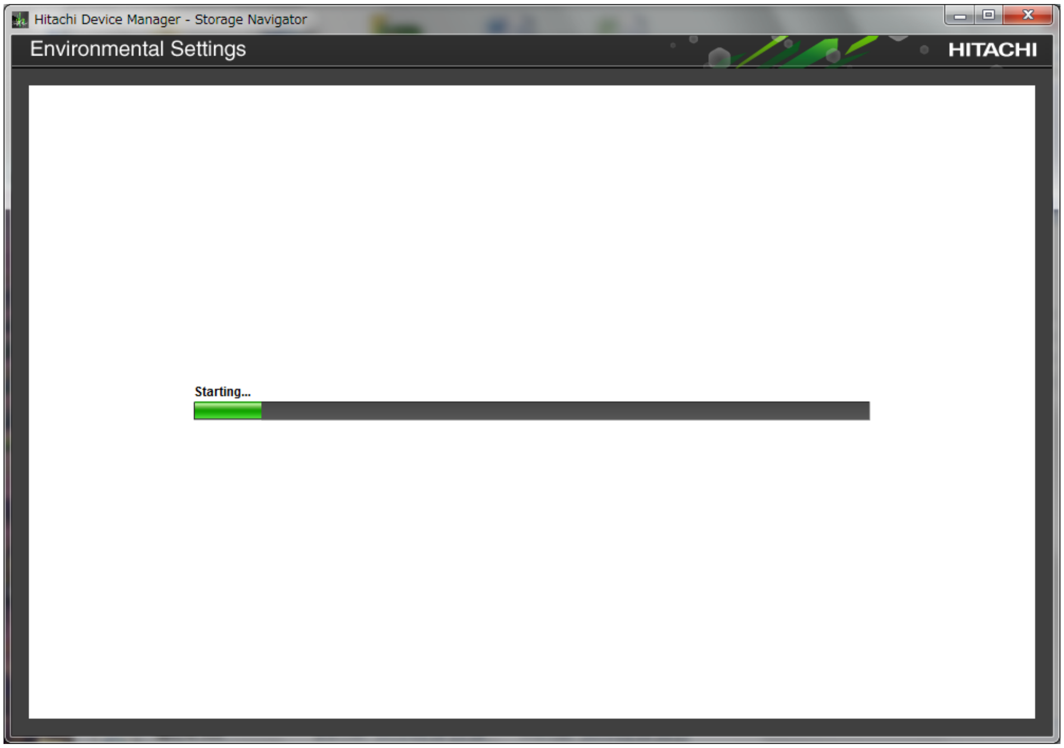
Install is completed.Set the below items.
(1)Port#
(2)Firewall
(3)Anti virus soft
you must start up service processes of Storage Navigator, after

● The setting has been completed.I will continue installation and updating of the software.

○ The setting has been completed.I will install and update the software later.

○ The setting is not completed.I will install and update the software after I complete the setting.

The **Environmental Settings** window opens as the system prepares for the upgrade.



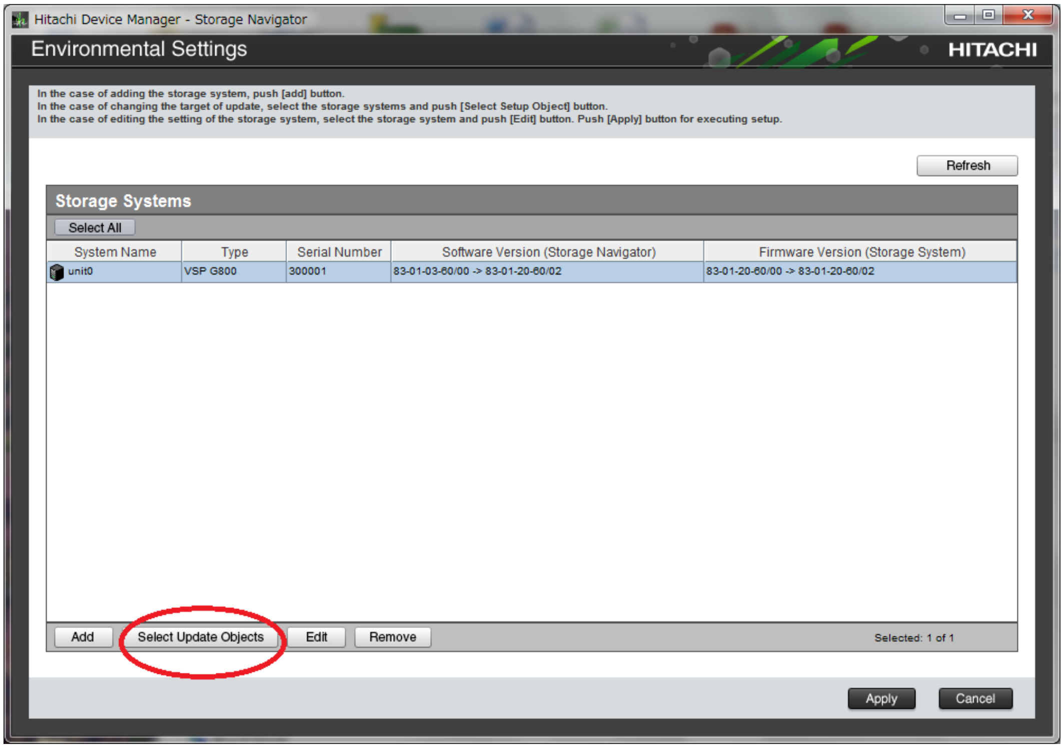
Hitachi Device Manager - Storage Navigator

Environmental Settings

Starting...

5. Wait for the preparation to complete and for the target storage systems list window to open.

6. When the target storage systems list window opens, select the appropriate storage systems, and then click **Select Update Objects**.

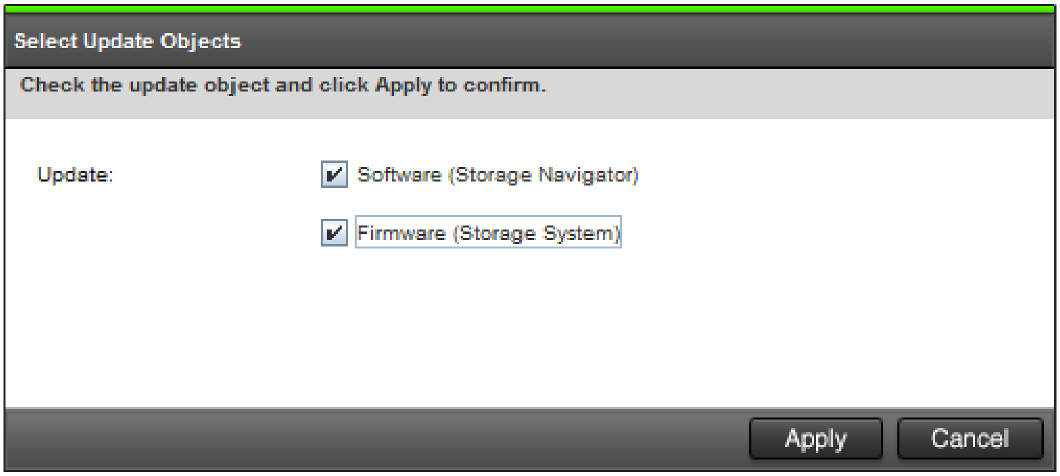


In the case of adding the storage system, push [add] button.
In the case of changing the target of update, select the storage systems and push [Select Setup Object] button.
In the case of editing the setting of the storage system, select the storage system and push [Edit] button. Push [Apply] button for executing setup.

System Name	Type	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
unit0	VSP G800	300001	83-01-03-60/00 -> 83-01-20-60/02	83-01-20-60/00 -> 83-01-20-60/02

The **Select Update Objects** window opens.

7. In the **Select Update Objects** window, select **Software (Storage Navigator)** and **Firmware (Storage Navigator)**.

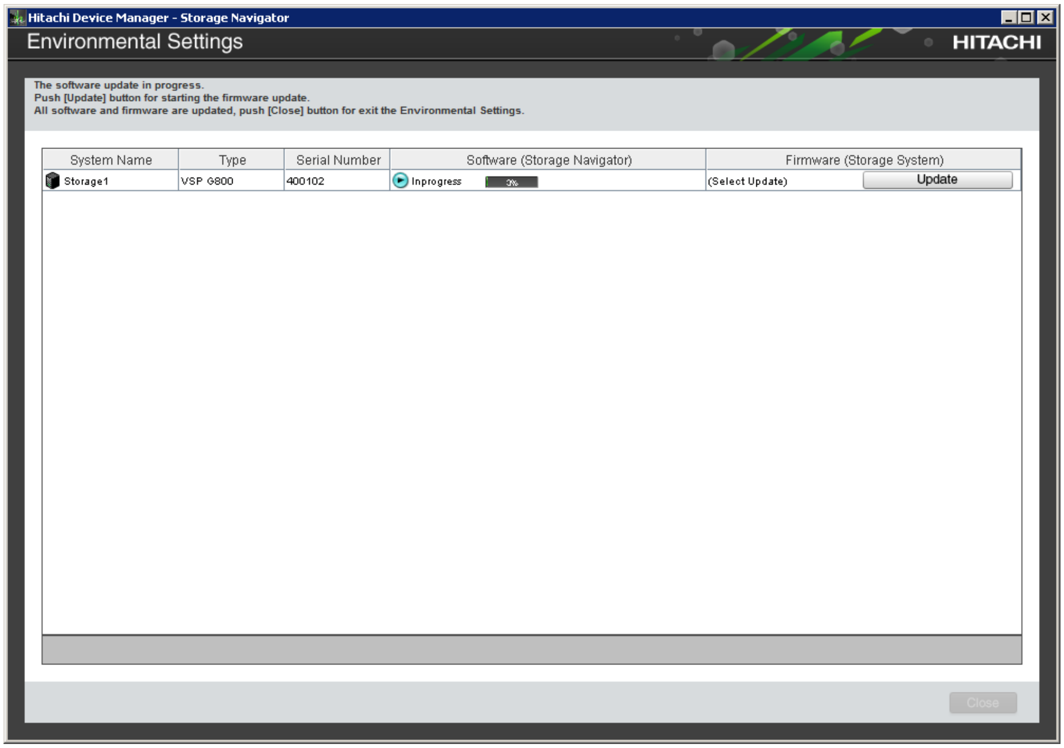


Check the update object and click Apply to confirm.

Update: ☑ Software (Storage Navigator)
☑ Firmware (Storage System)

8. Click **Apply**.
The **Update software and firmware** window opens.

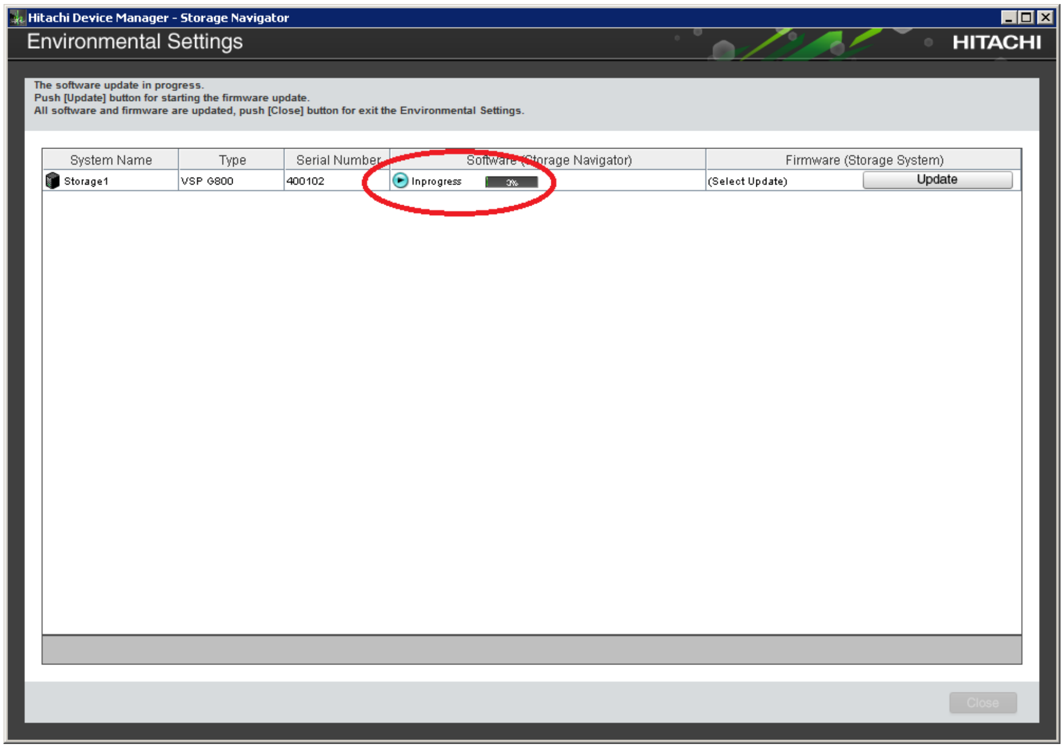
9. Click **Confirm**.
The **Run update** window opens and the software update starts automatically.



The software update in progress.
Push [Update] button for starting the firmware update.
All software and firmware are updated, push [Close] button for exit the Environmental Settings.

System Name	Type	Serial Number	Software (Storage Navigator)	Firmware (Storage System)
Storage1	VSP G800	400102	Inprogress 3%	(Select Update) Update

10. Verify the upgrade status in the **Software (Storage Navigator)** row.



The software update in progress.
Push [Update] button for starting the firmware update.
All software and firmware are updated, push [Close] button for exit the Environmental Settings.

System Name	Type	Serial Number	Software (Storage Navigator)	Firmware (Storage System)
Storage1	VSP G800	400102	Inprogress 3%	(Select Update) Update

Note:

Do not terminate the application forcibly while it is running otherwise, the message `[32061-208063]` might appear when you log on to the maintenance utility.

If the message displays, use the following corrective action:

a. Open the **Update Firmware** window from the newly opened **Maintenance Utility** window.

b. Verify the **Update Firmware** window is displaying. If the progress window appears, the firmware is currently updating. Wait until the firmware update is complete.

c. Perform the Force Release System Lock.

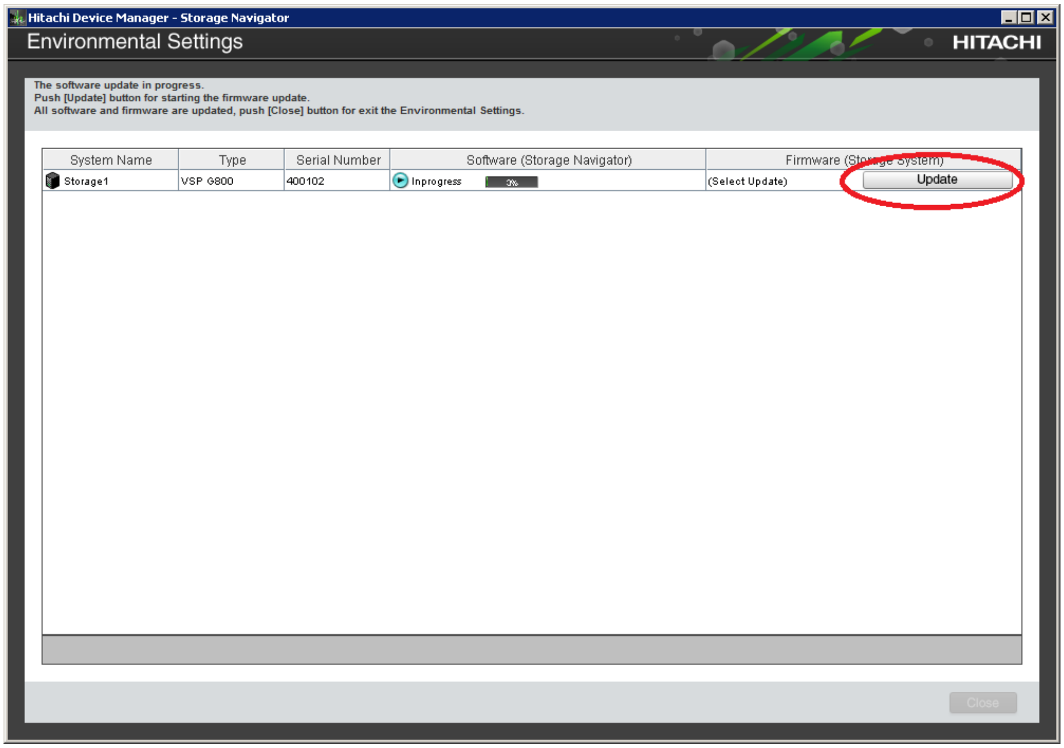
The following table shows the possible status conditions.

Status	Description
Waiting	Software waiting to be upgraded. Software components are upgraded individually.
In progress	Software is running.
Completed	Software upgrade is complete.
Failed	Software upgrade failed. Click **Update** to display the **Update Firmware** window and review the error details.
Communication Timeout	The completion of the firmware update in time[1] is not confirmed. Verify the state in the **Update Firmware** window.
(Not Update)	Not selected as a firmware upgrade target.
Note: 1. When NAS Modules are not installed, the installation time is approximately 3.5 hours. When NAS modules are installed, the installation time is approximately 9 hours.	

11. When the **Update software and firmware window** opens, click **Confirm**.

    The **Run Update Firmware** window opens and the upgrade starts automatically.

12. When the following window opens, click **Update**.

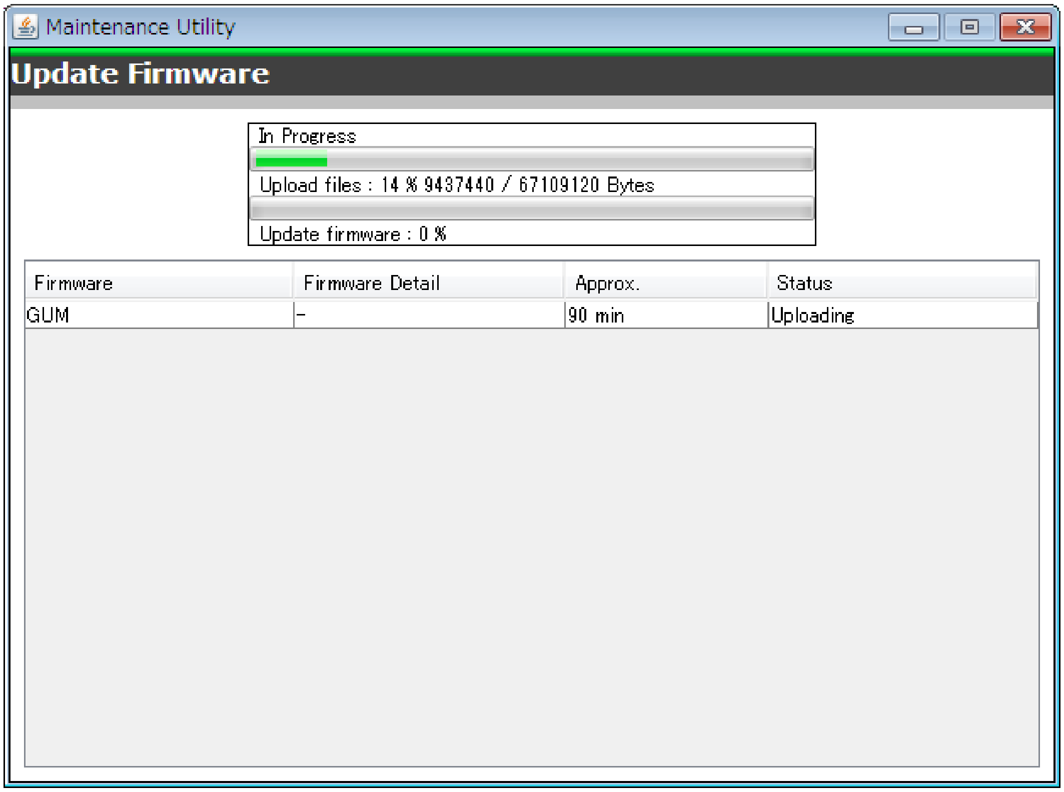


The software update in progress.
Push [Update] button for starting the firmware update.
All software and firmware are updated, push [Close] button for exit the Environmental Settings.

System Name	Type	Serial Number	Software (Storage Navigator)	Firmware (Storage System)
Storage1	VSP G800	400102	Inprogress 0%	(Select Update) Update

> **Note:** If a window reports a problem with this website security certificate, click **Continue to this website**, and then close the browser. If a **Java Update Needed** window opens, click **Later**. If a **JRE Security Warning** window opens, select the check boxes in each window and click **Continue**, **Run**, or **Yes**.

13. During the upgrade, the **Update Firmware** window closes and the following window opens.



In Progress

Upload files : 14 % 9437440 / 67109120 Bytes

Update firmware : 0 %

Firmware	Firmware Detail	Approx.	Status
GUM	-	90 min	Uploading

14. When the **Maintenance Utility** window specifies the restart of the GUM, click **OK**.
15. In the **Environmental Settings** window, verify the firmware update status in **Firmware (Storage System)**. Wait for the firmware update to complete. The following table lists the status conditions.

Status	Description
(Select Update)	Click **Update** to display the **Update Firmware** window.
In Progress	The **Update Firmware** window started and the firmware upgrade is not complete. This status appears even if the firmware upgrade is canceled.
Completed	Firmware upgrade is complete.
Failed	Firmware upgrade failed. Click **Update** to display the **Update Firmware** window and review the error details.
Communication Timeout	The time[1] required to complete the firmware upgrade cannot be confirmed. Verify the state in the **Update Firmware** window.
(Not Update)	Not selected as a firmware upgrade target.
Note: 1. When NAS Modules are not installed, the installation time is approximately 3.5 hours. When NAS modules are installed, the installation time is approximately 9 hours.	

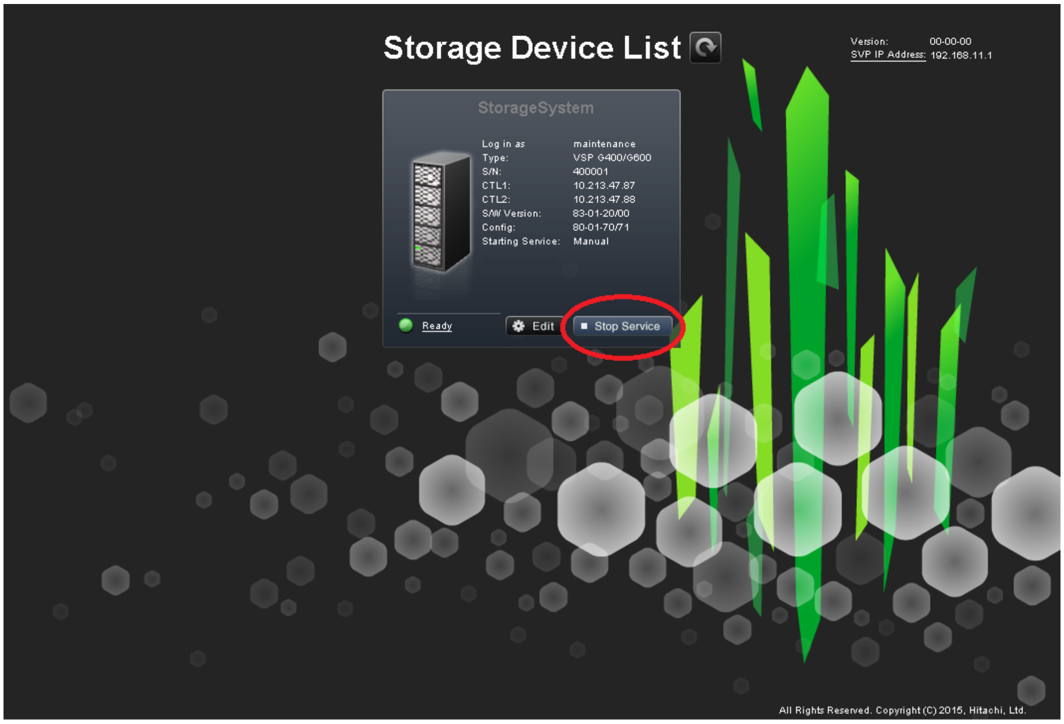
16. In the **Environmental Settings** window, click **Close**.
17. At the **Confirm exit** window, click **Confirm**.

Stopping the SVP service

Before upgrading the SVP software, stop the SVP service.

Procedure

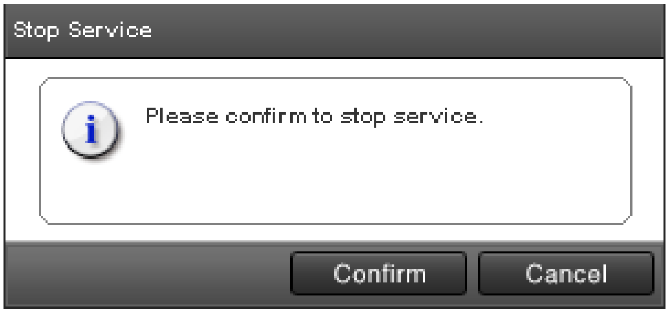
1. Connect the management console PC attached to the SVP, connect to the SVP using Windows Remote Desktop Client.
2. On the SVP, click **Start** > **All Programs** > **Hitachi Device Manager-Storage Navigator** > **StorageDeviceList**.
   The **Storage Device List** window opens.
3. In the **Storage Device List** window, record the **S/W Version**:________________________________
4. Click the **Stop Service** button for the registered storage system in the **Storage Device List** window.



Version: 00-00-00
SVP IP Address: 192.168.11.1

Log in as maintenance
Type: VSP G400/G600
S/N: 400001
CTL1: 10.213.47.87
CTL2: 10.213.47.88
S/W Version: 83-01-20/00
Config: 80-01-70/71
Starting Service: Manual

5. In the confirmation message, click the **Confirm** button.



Please confirm to stop service.

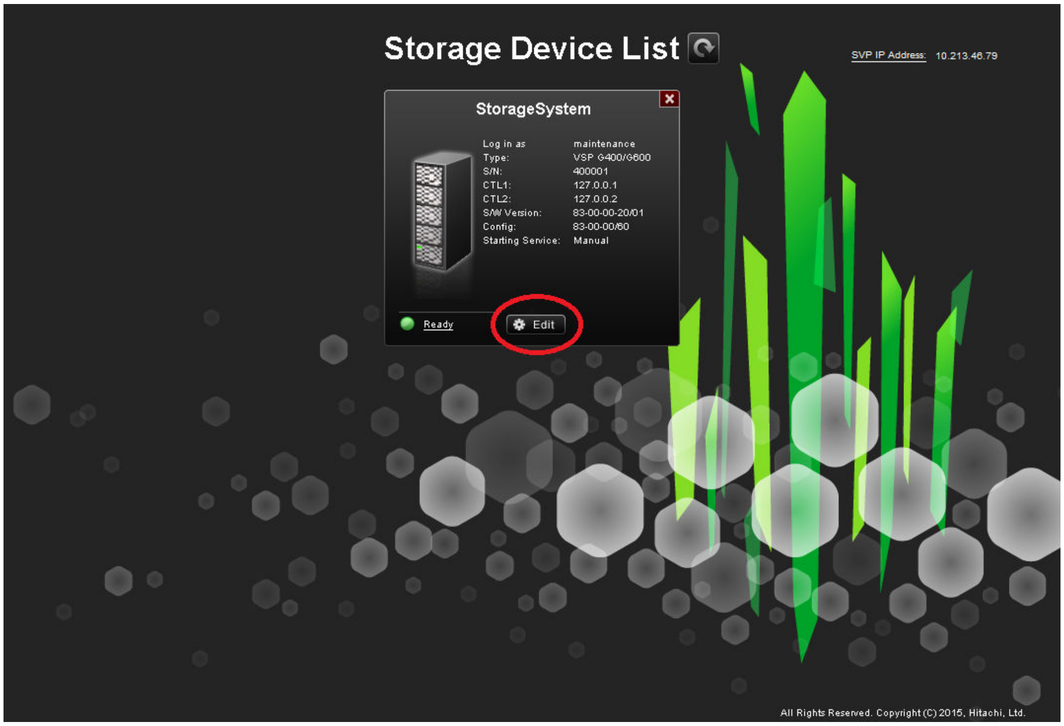
6. Proceed to Upgrading the software (on page 104) .

Upgrading the SVP software using Storage Device List

After stopping the SVP service, upgrade the SVP software. You can specify the SVP service to restart when the SVP is restarted. Store the new SVP software file in a location that can be accessed by the PC.

Procedure

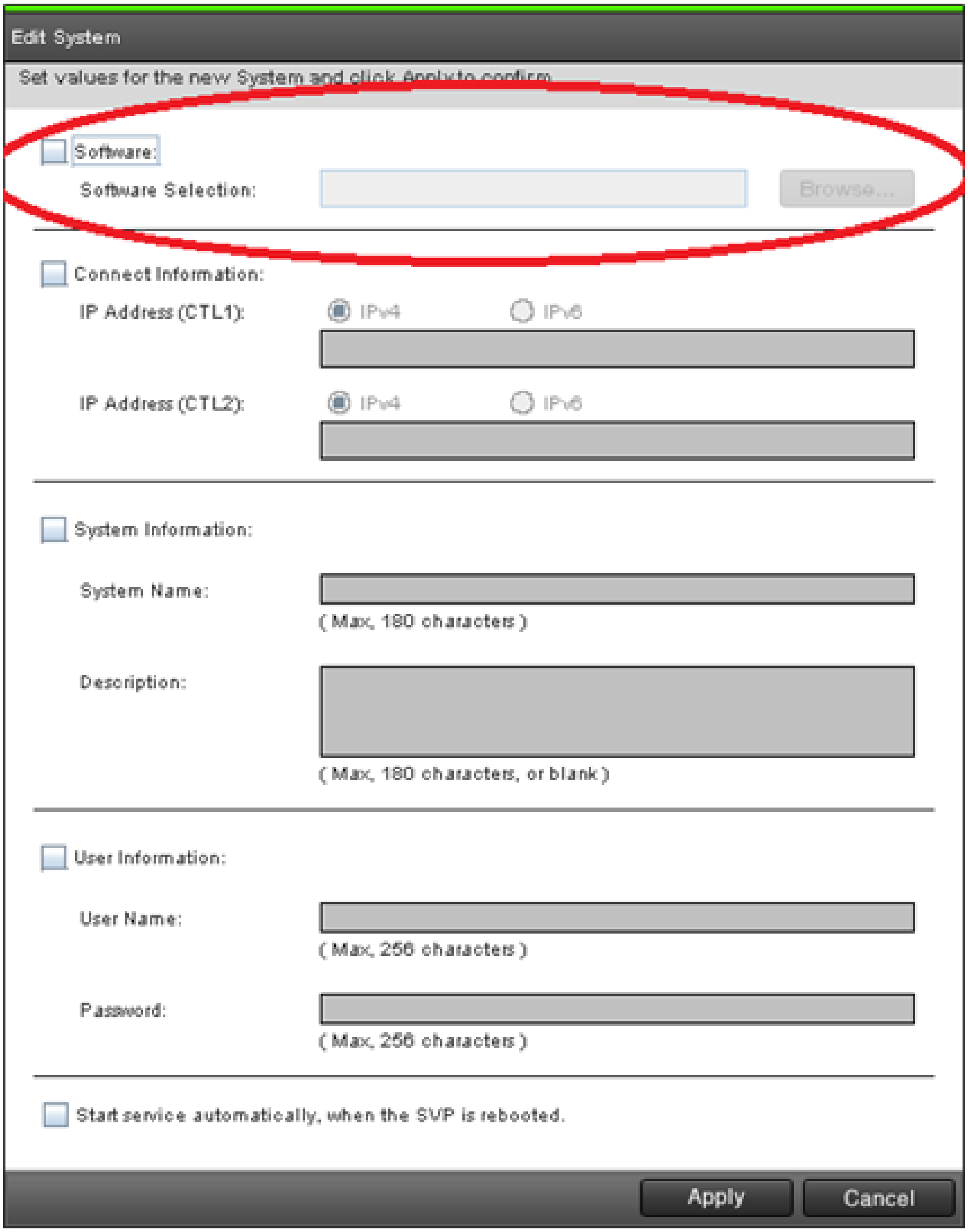
1. On the SVP, click **Start** > **All Programs** > **Hitachi Device Manager-Storage Navigator** > **StorageDeviceList**.
   The **Storage Device List** window opens.
2. In the **Storage Device List** window, click **Edit** for the storage system whose SVP software you want to upgrade.



SVP IP Address: 10.213.46.79

Log in as	maintenance
Type:	VSP G400/G600
S/N:	400001
CTL1:	127.0.0.1
CTL2:	127.0.0.2
S/W Version:	83-00-00-20/01
Config:	83-00-00/60
Starting Service:	Manual

3. In the **Edit System** window, select **Software** and click **Browse**.



Edit System

Set values for the new System and click Apply to confirm.

□ Software:

Software Selection: Browse...

□ Connect Information:

IP Address (CTL1): ● IPv4 ○ IPv6

IP Address (CTL2): ● IPv4 ○ IPv6

□ System Information:

System Name: (Max. 180 characters)

Description: (Max. 180 characters, or blank)

□ User Information:

User Name: (Max. 256 characters)

Password: (Max. 256 characters)

□ Start service automatically, when the SVP is rebooted.

4. Go to the location where you downloaded the software file (for example, `Software\productname.inf`), click the software file, and then click **Open**.
5. At the bottom of the **Edit System** window, check **Start service automatically, when the SVP is rebooted**.
6. Click **Apply**.
7. In the **Storage Device List** window, verify that the software version shown is later than the version you recorded prior to the upgrade.

> **Note:** If the update firmware window does not appear while upgrading the software, close the error window, and then update the software again.

8. If you disabled the Hi-Track Remote Monitoring System, go to the Hi-Track website and enable it (see http://hitrack.hds.com).

Downgrading the SVP software

Before downgrading the SVP software, contact the customer support.

Chapter 10: Security patch and antivirus software

Windows and Antivirus Update Policies

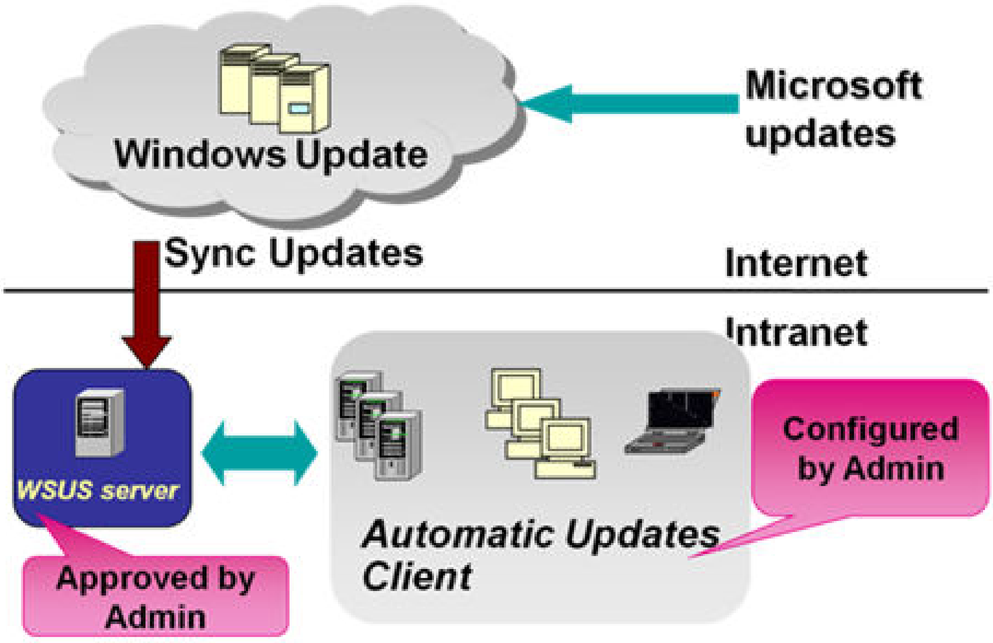
VSP G1000, VSP G1500, and VSP F1500 models

For the VSP G1000, VSP G1500 and VSP F1500 storage system models. The SVP is required by Hitachi Vantara in order to provide maintenance services to the systems. Only Hitachi Vantara representatives and authorized technicians are able to perform Windows and antivirus security updates to the SVP.

VSP Fx00 models and VSP Gx00 models

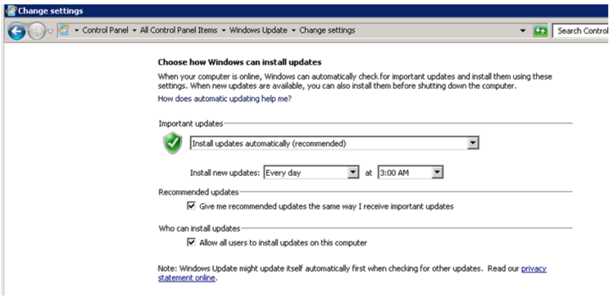
The customers can use the SVP to provision storage, connect with other management software, execute scripts, or for maintenance purposes. Hitachi Vantara does not require an SVP but, is available as an option, for the VSP G/F350, G/F370, G/F700, G/F900 models. However, the SVP is required for the VSP G200, G400, G600, G800 and VSP F400, F600, F800 models.

More importantly, Hitachi Vantara does not require access to the SVP and customers have full control over the security of the SVP machine credentials. Customers are responsible for applying Windows and antivirus security updates by using a Windows Server Update Services server or other acceptable methods.



Online update

Use automatic (recommended) or manual Windows updates to apply Microsoft security patches for storage systems configured for online environment.


Change settings
Control Panel ▸ All Control Panel Items ▸ Windows Update ▸ Change settings
Search Control

Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

How does automatic updating help me?

Important updates

Install updates automatically (recommended)

Install new updates: Every day at 3:00 AM

Recommended updates

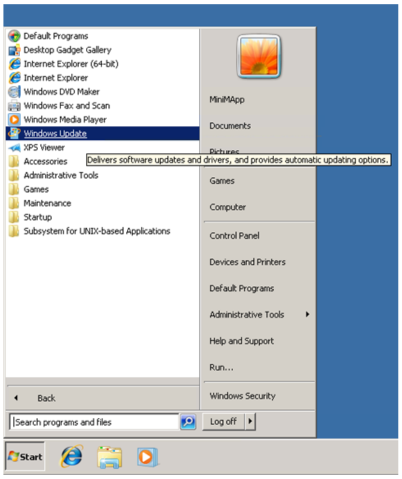
☑ Give me recommended updates the same way I receive important updates

Who can install updates

☑ Allow all users to install updates on this computer

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.

or



Delivers software updates and drivers, and provides automatic updating options.

Offline update

You can apply appropriate Windows security patches by downloading stand-alone packages from a Microsoft download site.

Operating system	Website
Windows 7	https://www.microsoft.com/EN-US/SEARCH/DOWNLOADRESULTS.ASPX?Q=WINDOWS+EMBEDDED+STANDARD+7&FIRST=11
	https://www.microsoft.com/EN-US/DOWNLOAD/DETAILS.ASPX?ID=41269
Windows 10 Professional and Windows 10 Enterprise	https://support.microsoft.com/en-us/help/4000825/windows-10-update-history
Windows Server 2012	https://www.microsoft.com/en-us/download/details.aspx?id=35626

Installing antivirus software on the SVP

Contact your Hitachi Vantara representative for specific required settings for your approved antivirus product.

For best practice, use one of the following antivirus software applications:

- Trend Micro OfficeScan Corporate Edition 10.6 / 11.0 / 11.0 SP1 / XG
- Symantec Endpoint Protection 14.0.0
- McAfee VirusScan Enterprise 8.8
- Sophos Endpoint Security and Control 10.3 / 10.6

For more information about support for antivirus applications, go to https://support.hitachivantara.com/en_us/user/tech-tips/e/2018april/T2018041301.html and log on to Support Connect.

⚠ **WARNING:** Installing antivirus software might affect SVP performance.

- Do not perform other maintenance operations. Doing so can delay processing or result in an error.
- Do not access the storage system or perform operations from remote sites using applications such as Hitachi Storage Navigator because it can delay processing or result in an error.
- When the SVP restarts during installation, data and logs monitored by the service information message or sense byte (SIM/SSB) might be interrupted temporarily.

Windows upgrade path

Item	Virtual Storage Platform and Unified Storage VM (HUS VM)	Virtual Storage Platform G1000 (VSP G1000) Virtual Storage Platform G1500 (VSP G1500) Virtual Storage Platform F1500 (VSP F1500)	VSP Gx00 models and VSP Fx00 models
Windows version	Windows Vista EOL April 2017	Windows 7 EOL January 2020	Windows 7 EOL January 2020
Hitachi Vantara supports Windows and antivirus maintenance	Yes	Yes	No
Upgrade path	VSP: Windows 7 (VSP) SVP does not support Windows 10 HUS VM: Windows 10	Windows 10	Windows 10
Customer billable	Yes	Yes	Yes
Additional information	The VSP SVP cannot upgrade from Windows 7 to Windows 10 due to limitations of the hardware. Please contact a Hitachi Vantara service provider.	New sales ship Windows 10 starting July 18, 2018 Windows 10 upgrade requires new SVP hardware	New sales ship Windows 10 starting May 8, 2018 Windows 10 upgrade requires new SVP hardware

Chapter 11: Setting up SSL encryption

You can set up a Secure Sockets Layer (SSL) connection to encrypt the Hitachi Device Manager - Storage Navigator user ID and password exchanged between the storage system and SVP.

About SSL

SSL is a protocol for transmitting data securely over the Internet. Two SSL-enabled peers use their private key and public key to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.

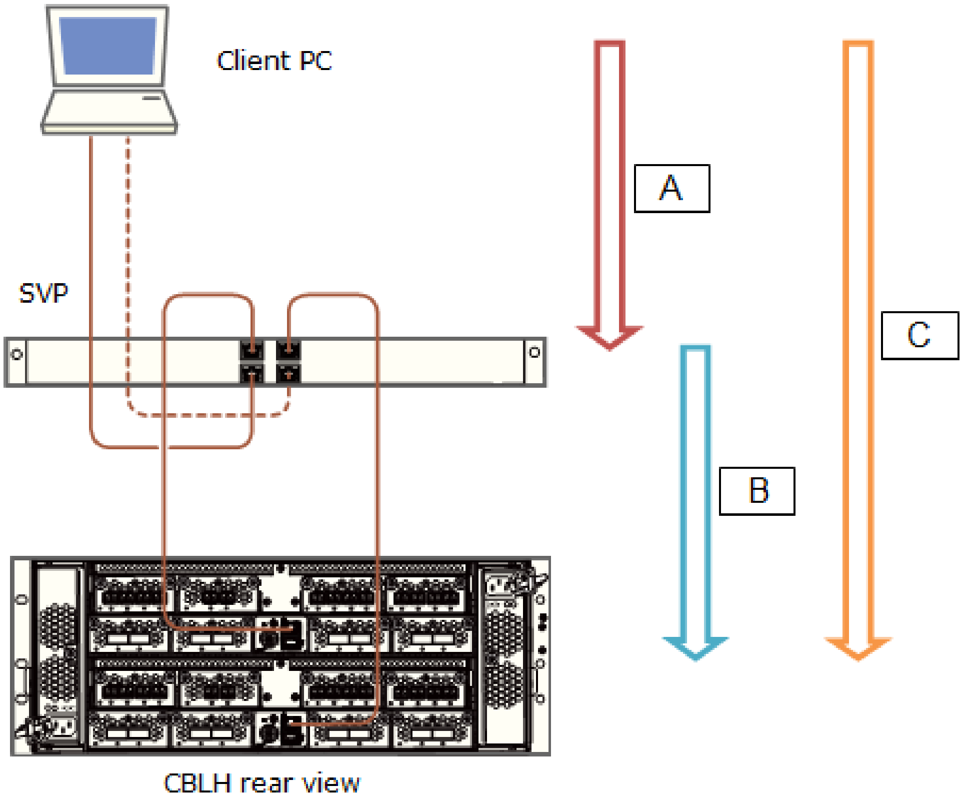
The following terms are associated with SSL:

- Keypair: A keypair is two mathematically related cryptographic keys consisting of a private key and its associated public key.
- Server certificate: A server certificate forms an association between an identity (in this case, the SVP server) and a specific public key and private key. A server certificate is used to identify the SVP server to a client, so that the server and client can communicate using SSL. Certificates can be self-signed or issued by a certificate authority (CA). Self-signed certificates are generated by you, and the subject of the certificate is the same as the issuer of the certificate. A client PC and SVP on an internal LAN behind a firewall might provide sufficient security. Certificates issued by the CA are signed and trusted server certificates, where a Certificate Signing Request (CSR) is sent to and certified by a trusted CA such as VeriSign. Using a certificate from a CA provides higher reliability than a self-signed certificate, but is also more expensive and can include several requirements.

SSL encryption of the storage system

The storage system uses SSL encryption for three connection paths. These paths are designated A to C in the following table and figure.

Connection path in figure	Connection path description	Encryption purpose	Certificate to be used
A	Between the SVP and client PC	Operation of Device Manager - Storage Navigator	A signed certificate of SSL encryption between the SVP and client PC
B	Between the SVP and storage system	SVP exchanges the information with the storage system	The certificate for "Connect to SVP" and the certificate for "Web server"
C	Between the client PC and storage system	Operation of maintenance utility	The certificate for "Web server"



To prevent a man-in-the middle attack, the encryption shown in notation B (between SVP and storage system) verifies the validity of the connection by using the certificate that was uploaded to the SVP in advance and by using the certificate of the storage system. The same certificate must be uploaded to the SVP and the storage system.

Note: If a certificate for the SVP or the storage system is changed, the SVP does not operate normally. Upload the certificate to the storage system before uploading the certificate to the SVP.

Different certificates can be used to connect to the SVP and web server.

Certificate	Upload destination	Comments
A signed certificate of SSL encryption between the SVP and client PC	SVP	N/A
For connecting to the SVP	SVP and storage system	If a certificate for the SVP or the storage system was uploaded, the SVP will not operate normally.
For connecting to the web server	SVP and storage system	If a certificate for the SVP or storage system was uploaded, the SVP will not operate normally.

Creating private and public keys requires a dedicated program, such as those you can download from the OpenSSL website.

Setting up SSL communications

In the following procedure, you create private and public keys using a dedicated program, such as those you can download form the OpenSSL website.

Procedure

1. Download OpenSSL.
2. Create a private key.
3. Create a public key.
4. Acquire a signed certificate.
5. Upload the signed SSL certificate.
6. Import the certificate into the web browser (optional).
7. Block HTTP communications.

Updating the SVP server certificate

Updating the SVP certificate renders some tasks temporarily unavailable.

- While the SVP server certificate is being updated, tasks that are being performed or scheduled to be performed on Device Manager - Storage Navigator are not executed.
- Certificates for RMI communication are updated asynchronously (within approximately two minutes).
- If an SVP certificate is updated during Hitachi Command Suite setup operation, the setup operation results in an error.
- Updating the SSL certificate may cause an SVP failure. Therefore exercise care to keep the certificate and private key consistent.
- After the certificate update completes, the SVP server can take 30 to 60 minutes to restart, depending on the environment. A long period of time can cause an internal server error without displaying the update completion dialog box does. Despite this behavior, the certificate update completes.

Creating a private key (.key file)

A private key is required to create an SSL keypair.

Procedure

1. Download and install the `openssl.exe` file from the OpenSSL website.
   In the following example, the `openssl.exe` file is installed to the `c:\openssl` folder.
2. If the read-only attribute is set, remove this attribute from the `c:\openssl` folder.
3. Open a command prompt.
4. Move the current directory to the folder to which the key file is output, such as `c:\key`.
5. Execute the following command: `c:\key > c:\openssl\bin\openssl genrsa -out server.key 2048`
   A file called `server.key` is created in the `c:\key` folder. This file becomes the private key.

Creating a public key (.csr file)

A public key is required to create an SSL keypair.

Procedure

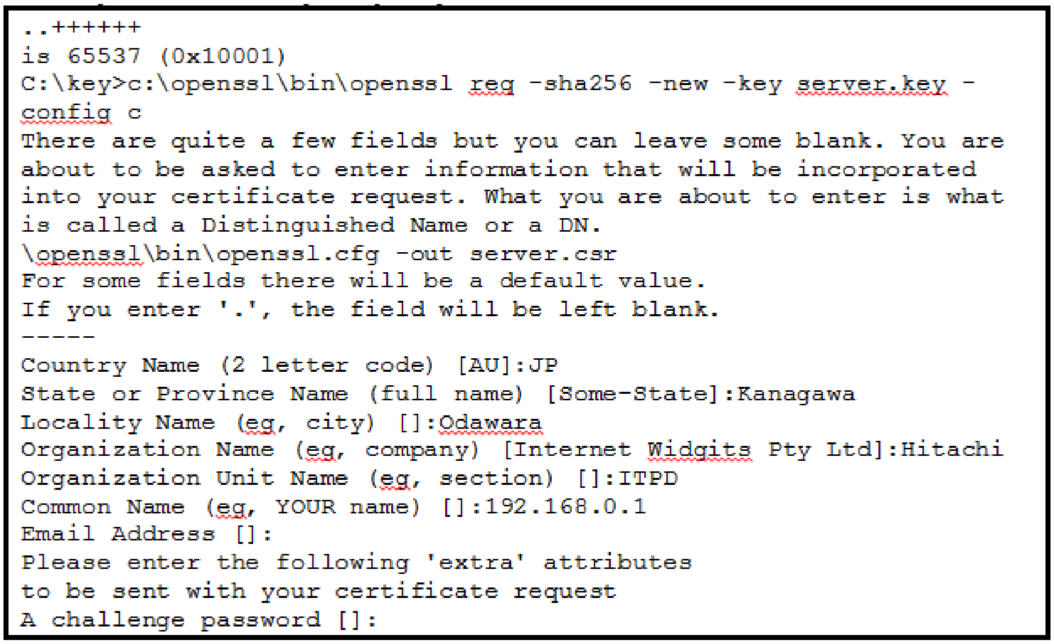
1. Open a command prompt and issue the following command: `C:\key > c:\openssl\bin\openssl req -sha256 -new -key server.key –config c:\openssl\bin\openssl.cfg -out server.csr`

This command uses SHA-256 as a hash algorithm. The `server.csr` file is created in the `C:\key` folder as a public key.

> **Note:** Do not use MD5 or SHA-1 for a hash algorithm due to its low security level. Use SHA-256 for a hash algorithm.

2. Enter the following information in the prompt:
   - Country Name (two-letter code)
   - State or Province Name
   - Locality Name
   - Organization Name
   - Organization Unit Name
   - Common Name
   - To create a self-signed certificate, enter the IP address of the server (SVP). The name you entered here is used as the server name (host name). To obtain a signed and trusted certificate, verify that the server name matches the host name of the SVP.
   - Email Address
   - Challenge password (optional)
   - Company name (optional)

   The following example shows a sample command prompt input.



```
..++++++
is 65537 (0x10001)
C:\key>c:\openssl\bin\openssl req -sha256 -new -key server.key -
config c
There are quite a few fields but you can leave some blank. You are
about to be asked to enter information that will be incorporated
into your certificate request. What you are about to enter is what
is called a Distinguished Name or a DN.
\openssl\bin\openssl.cfg -out server.csr
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
Locality Name (eg, city) []:Odawara
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hitachi
Organization Unit Name (eg, section) []:ITPD
Common Name (eg, YOUR name) []:192.168.0.1
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

Acquiring a signed certificate for the private key

After creating a private key and a public key, acquire a signed certificate file for the public key.

There are three ways to acquire a signed certificate:

- Create a certificate by self-signing.
- Acquire a certificate of certificate authority that is used within your company.
- Acquire an official certificate by requesting one from a CA.

When you send a request to a certificate authority, specify `SVP` as the host name. There will be an extra charge.

Best practice is to use self-signed certificates only when testing encrypted communication.

To acquire a self-signed certificate:

Procedure

1. Open a command prompt.
2. Issue the following command: `c:\key>c:\openssl\bin\openssl x509 -req -sha256 -days 10000 -in server.csr -signkey server.key -out server.crt`
   The validity period is set 10,000 days as an example. This command uses SHA-256 as a hash algorithm.

   > **Note:** Do not use MD5 or SHA-1 for a hash algorithm due to its low security level. Use SHA-256 for a hash algorithm.

Acquiring a signed and trusted certificate

To acquire a signed and trusted certificate, you must acquire a CSR, send that file to a CA, and request the CA to issue a signed and trusted certificate.

Each certificate authority has its own procedures and requirements, and there is generally a cost for doing so. The signed and trusted certificate is the signed public key.

Removing the passphrase from an SSL certificate

You cannot upload a passphrase-protected SSL certificate to the SVP. Before uploading a SSL certificate to the SVP, remove the passphrase from the SSL certificate.

The following procedure describes how to verify whether the passphrase is set and how to remove it.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. To verify a passphrase, move to the current directory to the folder (for example, `C:\key`) to store the key file, and then issue the following command:
   `C:\key>c:\openssl\bin\openssl rsa -in [input_key_file] -out [output_key_file]`

   > **Note:** If you issue this command, the key file is overwritten. Therefore, best practice is to back up a key file in advance and prepare the output or input directory of the key file separately.

3. You cannot upload a passphrase-protected SSL certificate to the SVP. Enter the passphrase that has been set and remove it using the command to verify a passphrase: `C:\key>c:\openssl\bin\openssl rsa –in server.key –out server.key Enter pass phrase for server.key: Enter the passphrase. Writing RSA key`
4. If the path phrase entry is not required for the path phrase confirmation command, you can upload a SSL certificate to the SVP :
   a. Issue the following command: `C:\key>c:\openssl\bin\openssl rsa -in [input_key_file] -out [output_key_file].`
   b. Press the Enter key.
   c. Issue the following command: `Writing RSA key`.
5. Verify that the path phrase is released, and then close the command prompt.

Converting the SSL certificate into the PKCS#12 format

When uploading the created private key and the SSL certificate to the storage system, you must convert the certificate into the PKCS#12 format. If the SSL certificate is not uploaded to the storage system, the conversion is unnecessary.

> **Note:** In this procedure, the file name of the private key is set as `client.key` and the file name of the SSL certificate, `client.crt`. In addition, the SSL certificate file in the PKCS#12 format is output to `c:\key`.

This procedure assumes that the private key and the SSL certificate are stored in the same folder, and that all users are logged out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. Issue the following command: `C:\key>c:\openssl\bin\openssl pkcs12 -export -in client.crt -inkey client.key -out client.p12`

3. Enter an arbitrary password. This password is used when uploading the SSL certificate in the PKCS#12 format to the storage system. The characters used for the password when creating the SSL certificate in the PKCS#12 format are shown as follows. and specified by the character string of 128 characters or less: A-Z a-z 0-9 ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ `{ | } ~
   The `client.p12` file is created in the `C:\key` folder. This file is the SSC certificate converted into the PKCS#12 format.
4. Close the command prompt.

Uploading the signed server certificate of the SSL communication between the SVP and client PC

Upload the private key and the signed server certificate (public key) to the SVP for using an arbitrary certificate for SSL communications between the SVP and client PC.

The following describes how to upload the certificate using the certificate update tool. This procedure assumes that:

- A private key (`server.key` file) has been created. Change the file name to `server.key` unless the file already uses that name.
- A signed public key certificate (`server.crt` file) has been acquired. Change the file name to `server.crt` unless the file already has that name.
- All users are logged out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the directory where the certificate update tool (`MappApacheCrtUpdate.bat`) is located. Issue the following command: `C:\MAPP \wk\Supervisor\MappIniSet\ MappApacheCrtUpdate.bat r[absolute path of the certificate file] r[absolute path of the private key file]`.

   Note: `C:\MAPP` indicates the installation directory of the SVP. If you specify an installation directory other than `C:\Mapp`, replace `C:\Mapp` with the specified installation directory.

3. At the message `Press any key to continue the process`..., enter an arbitrary key.
4. Close the command prompt.

Returning the certificate of the SSL communication between the SVP and the client PC to the default

This procedure requires all users to log out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, start a Windows command prompt as an Administrator.
2. Move the current directory to the directory where the tool (`MappApacheCrtInit.bat`) is located. Issue the following command: `C:\MAPP\wk\Supervisor\MappIniSet\ MappApacheCrtInit.bat`

   > **Note:** `C:\MAPP` indicates the installation directory of the SVP. If you specify an installation directory other than `C:\Mapp`, replace `C:\Mapp` with the specified installation directory.

3. At the message `Press any key to continue the process…`, enter an arbitrary key.
4. Close the command prompt.

Uploading the certificate to the SVP

To you use an arbitrary certificate for SSL communications between the SVP and storage system, upload the private key and the signed server certificate (public key) to the SVP.

This procedure assumes that:

- The private key of the storage system and the signed server certificate (public key) from the maintenance utility have been updated.
- The private key (`server.key` file) and the signed public key certificate (`server.crt` file) are in the X.509 PEM or X.509 DER format.
- All users are logged out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the directory where the certificate update tool (`MappL7SwitchGumSslCrtUpdate.bat`) is located. Issue the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\
   MappL7SwitchGumSslCrtUpdate.bat r[absolute path of the
   certificate file]
   ```

   > **Note:** `C:\MAPP` indicates the installation directory of the SVP. If you specify an installation directory other than `C:\Mapp`, replace `C:\Mapp` with the specified installation directory.

3. At the message `Press any key to continue the process…`, enter an arbitrary key.
4. Close the command prompt.

Uploading the certificate to the web server

Execute the SSL communication with Device Manager - Storage Navigator installed on the SVP as a client and the controller of the storage system as a server. Upload the private key and the signed server certificate (public key) to the SVP for using the SSL communication. The following describes how to upload the certificate using the certificate update tool.

This procedure assumes that:

- The private key of the storage system and the signed server certificate (public key) for the web server from the maintenance utility have been updated.
- The private key (`server.key` file) and the signed public key certificate (`server.crt` file) are in X.509 PEM or X.509 DER format.
- All users are logged out of Device Manager - Storage Navigator.

Procedure

1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the directory where the certificate update tool (`MappSn2GumSslCrtUpdate.bat`) is located. Issue the following command:
   ```
   C:\MAPP\wk\Supervisor\MappIniSet\ MappSn2GumSslCrtUpdate.bat
   r[absolute path of the certificate file]
   ```

   Note: `C:\MAPP` indicates the installation directory of the SVP. If you specify an installation directory other than `C:\Mapp`, replace `C:\Mapp` with the specified installation directory.

3. At the message `Press any key to continue the process`…, enter an arbitrary key.
4. Close the command prompt.

Returning the web server certificate to the default

If necessary, you can revert to the default web server certificate.

This procedure assumes that:

- The private key (`server.key` file) and the signed public key certificate (`server.crt` file) are in X.509 PEM or X.509 DER format.
- All users are logged out of Device Manager - Storage Navigator.

Procedure

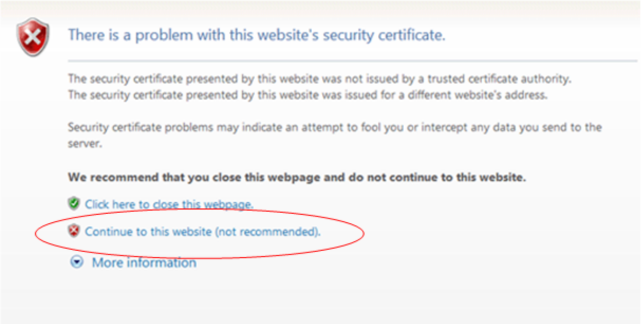
1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the directory where the certificate update tool (`MappSn2GumSslCrtInit.bat`) is located. Issue the following command: `C:\MAPP\wk\Supervisor\MappIniSet\MappSn2GumSslCrtInit.bat`

> **Note:** `C:\MAPP` indicates the installation directory of the SVP. If you specify an installation directory other than `C:\Mapp`, replace `C:\Mapp` with the specified installation directory.

3. At the message `Press any key to continue the process…`, enter an arbitrary key.
4. Close the command prompt.

Resolving security certificate messages

When starting an SSL-enabled Device Manager - Storage Navigator session, the following message appears if the security certificate was not issued by a trusted certificate authority. If the following alert message appears, click **Continue to this website (not recommended)**.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Blocking HTTP communications to the SVP

You can block outside access to the HTTP communication port used by the SVP.

Procedure

1. Request all users to log out of HDvM - SN.
2. Using a management console PC attached to the SVP, connect to the SVP using Windows Remote Desktop Client.
3. On the SVP, exit to a Windows command prompt as Administrator.
4. Move to the directory where the `MappHttpBlock.bat` tool is located, and then issue the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappHttpBlock.bat
   ```

   In this command, `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is different, replace `C:\MAPP` with the specified installation directory.

5. At the message `Press any key to continue the process…`, press any key, and then close the command prompt window.

Releasing HTTP communications to the SVP

If you blocked outside access to the HTTP communications used by the SVP, use the following procedure to release the blocked port.

Procedure

1. Request all users to log out of HDvM - SN.
2. Using a management console PC attached to the SVP, connect to the SVP using Windows Remote Desktop Client.
3. On the SVP, exit to a Windows command prompt as Administrator.
4. Move to the directory where the `MappHttpBlock.bat` tool is located, and then enter the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappHttpRelease.bat
   ```

   In this command, `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is different, replace `C:\MAPP` with the specified installation directory.
5. At the message `Press any key to continue the process`..., enter a port number that is not being used by another device or application.
6. Close the command prompt window.

Chapter 12: Changing the storage IP address

There might be times when you need to change the storage system's IP address. For convenience, there are two ways to change the IP address: using the maintenance utility on the SVP and using the Storage Device List.

Using the SVP to set the storage system IP address

You can use the maintenance utility on the SVP to configure an IP address for the storage system.

⚠ **Caution:** Do not connect network servers such as the proxy between the client PC, SVP, and the storage system.

Before you begin

Verify the storage system, SVP, and client PC are attached to the SVP and all are on the same subnet.

- Default IP address for controller 1 user LAN port: 192.168.0.16
- Default IP address for controller 2 user LAN port: 192.168.0.17
- Subnet mask: 255.255.255.0

Procedure

1. Start the SVP, and then log on to it.
2. Configure the SVP to use a temporary port of `192.168.0.xxx`, where `xxx` is a number from 1 to 254, excluding 16 and 17.
3. Launch a web browser.
4. In the address bar, enter the IP address of controller 1.

   When NAS modules are installed, the window for selecting Maintenance Utility or NAS Manager is displayed. Select **Maintenance Utility**.

   The **Maintenance Utility** logon window opens.
5. Log on to the maintenance utility using a user account that has administrative privileges.
6. The first time you log on to the maintenance utility, enter a password for the user account:
   a. On the **Maintenance** menu, click **System Management** > **Change Password**.
   b. Enter a password.
   c. Click **Finish**.

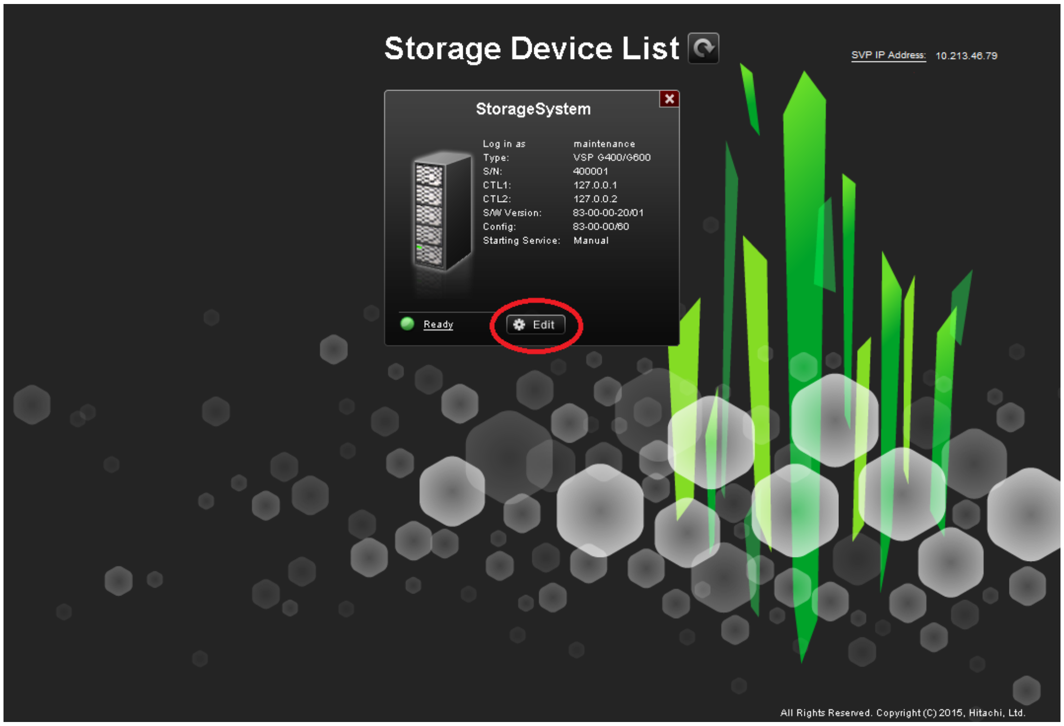
7. Set the user IP address.
   a. On the **Maintenance Utility** menu, click **Network Settings**.
   b. In the **Network Settings** window, click **Set Up Network Settings**.
   c. Set the IP address for controller 1 and controller 2.
   d. Click **Apply**.
8. Click **Log Out** to close the maintenance utility.
9. Change the storage system IP address in the **Storage Device List** window.
10. Set the SVP IP address.
11. Change the SVP IP address in the **Storage Device List**.
12. If you assigned a temporary IP address to the client PC, change it to meet the subnet of your network environment.

> **Note:** If you encounter a problem, troubleshoot the spanning tree protocol.

Changing storage system information in the Storage Device List

Procedure

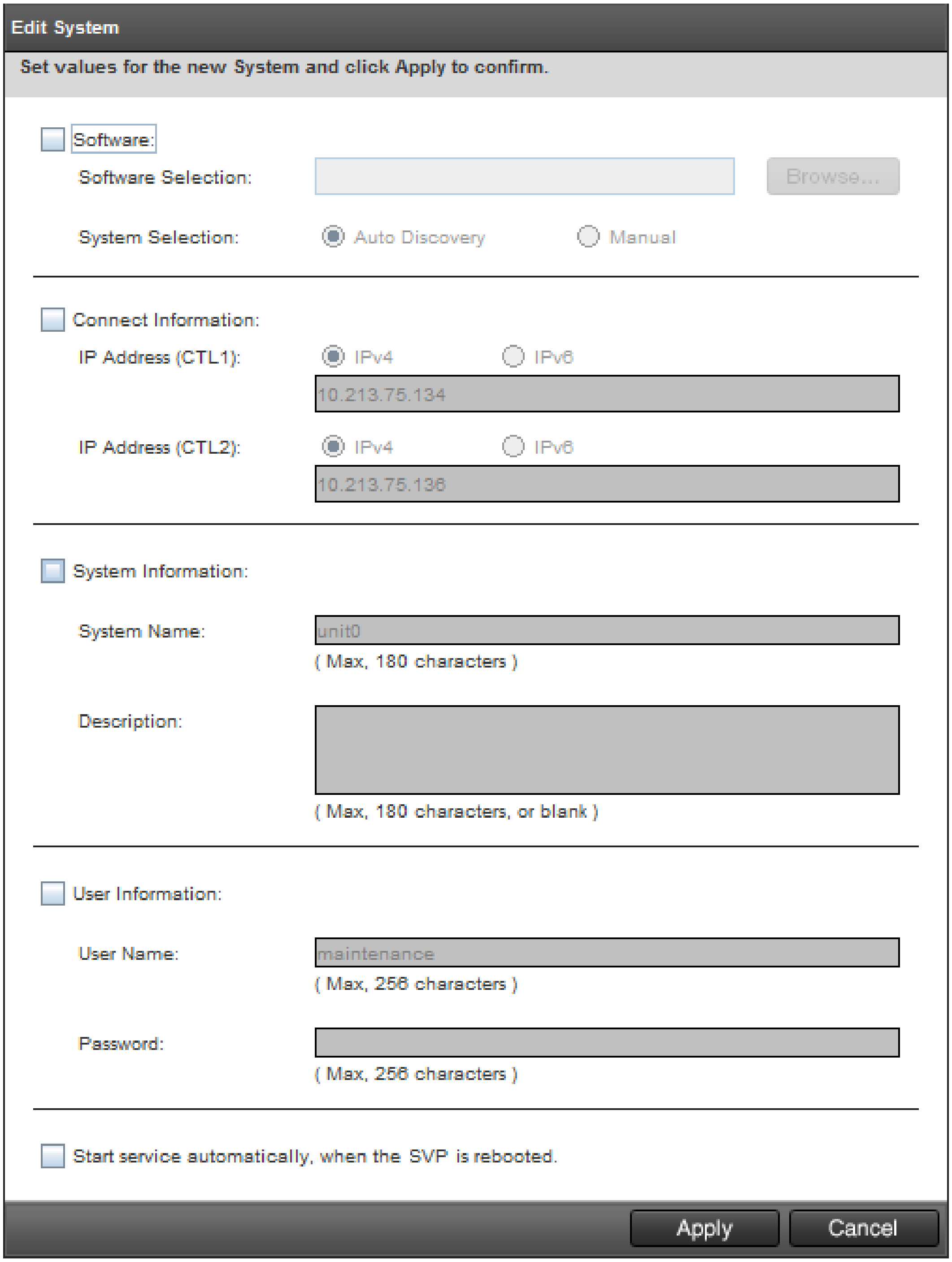
1. In the **Storage Device List** window, click the **Edit** button for the storage system you want to edit.



SVP IP Address: 10.213.46.79

Log in as maintenance
Type: VSP G400/G600
S/N: 400001
CTL1: 127.0.0.1
CTL2: 127.0.0.2
S/W Version: 83-00-00-20/01
Config: 83-00-00/60
Starting Service: Manual

The **Edit System** window opens.



Edit System

Set values for the new System and click Apply to confirm.

□ Software:

Software Selection: Browse...

System Selection: ● Auto Discovery ○ Manual

□ Connect Information:

IP Address (CTL1): ● IPv4 ○ IPv6

10.213.75.134

IP Address (CTL2): ● IPv4 ○ IPv6

10.213.75.136

□ System Information:

System Name: unit0

(Max, 180 characters)

Description:

(Max, 180 characters, or blank)

□ User Information:

User Name: maintenance

(Max, 256 characters)

Password:

(Max, 256 characters)

□ Start service automatically, when the SVP is rebooted.

2. Enter the items to be changed, and then click **Apply**.

> **Note:** To change **Software**, do not select **Manual** of **System Selection** to set it. Clear **Start service automatically, when the SVP is rebooted** check box when:
>
> - Storage systems running **S/W Version** 83-01-xx or later are registered.
> - Multiple storage systems are registered.

Chapter 13: Changing the SVP IP address

You can use Windows OS on the SVP or the Storage Device list to change the IP address of the SVP.

Changing the SVP IP address in Windows

⚠ **Caution:** Do not connect network servers such as the proxy between the client PC, SVP, and the storage system.

Use this procedure if a storage system is not registered on the SVP or the storage system service has not started.

Procedure

1. On the SVP, click **Start** > **Control Panel** > **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Click a network for which you want to set an IP address, and then set the IP address.

Changing the SVP IP address using Storage Device List

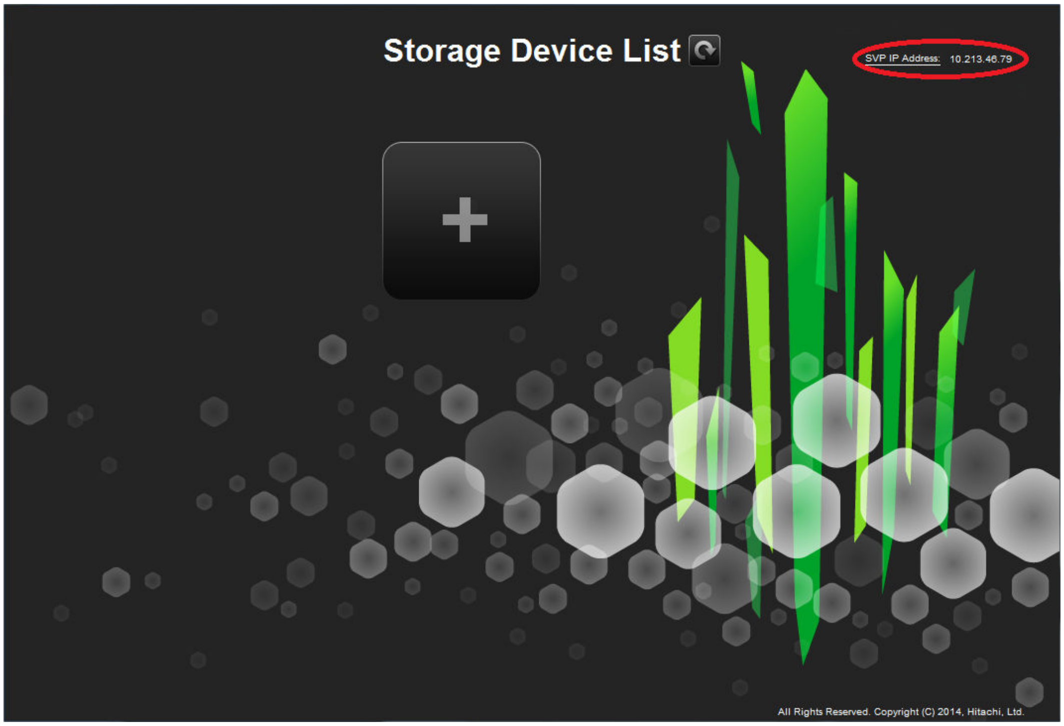
To change the SVP IP address in Storage Device List, change the IP address registered using the SVP's Windows operating system, and then perform the following procedure.

Before you begin

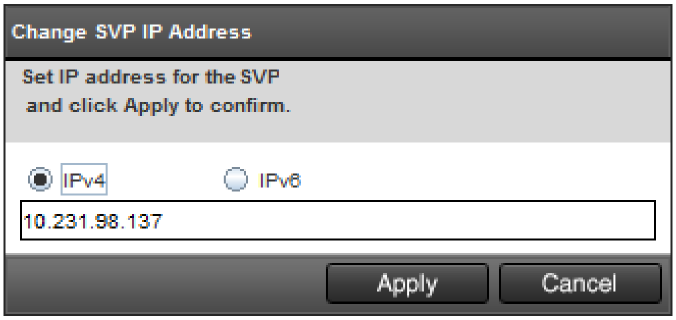
- Do not register the storage system on the SVP.
- Stop the service of the storage system.

Procedure

1. On the SVP, click **Start** > **All Programs** > **Device Manager - Storage Navigator** > **StorageDeviceList**.
   The **Storage Device List** window opens.
2. In the top-right side of the window, click **SVP IP Address**.


Storage Device List
SVP IP Address: 10.213.46.79
+
All Rights Reserved. Copyright (C) 2014, Hitachi, Ltd.

The **Change SVP IP Address** window opens.



Change SVP IP Address

Set IP address for the SVP
and click Apply to confirm.

● IPv4 ○ IPv6

10.231.98.137

3. Click **IPv4** or **IPv6**.
4. Enter the new IP address of the SVP.
5. Click **Apply**.

Chapter 14: Changing and initializing SVP port numbers

If other applications are using the port numbers used by the SVP, change the SVP port numbers. You can also revert the SVP port numbers to their original settings if necessary.

Changing SVP port numbers

You can change the SVP port numbers in supported applications. If you use a firewall, change and apply your firewall settings before you change the SVP port numbers. Unused port numbers are automatically allocated for some port numbers of the SVP software with SVP software version later than 83-03-01-xx/00.

Before you begin

Verify the client PC is already connected to the SVP through Remote Desktop Connection.

Procedure

1. Request all users to log out of Device Manager - Storage Navigator.
2. On the SVP, exit to a Windows command prompt as Administrator.
3. Change to the directory to the location of the tool `MappSetPortEdit.bat`.
4. Enter the following command: `C:\Mapp\wk\Supervisor\MappIniSet\MappSetPortEdit.bat _ [port number key name] _ [port number]` where _ indicates a space and the values [ ] indicate a parameter. For example:

   ```
   >cd C:\Mapp\wk\Supervisor\MappIniset\mappsetportedit.bat
   MAPPWebServer 10001
   ```

   > **Note:** In this command, `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with the appropriate installation directory.

The following table shows the port numbers you can use. The communication direction is outbound between the client PC to the SVP.

Note: Refer to the following table for port number assignments if the storage system is using a physical service processor.

Port number key name (Windows Firewall Inbound name)	Protocol	Initial value of port number	Can the port be closed?	SVP software version
MAPPWebServer	HTTP	80	Yes	83-01-20-xx/00 or later
MAPPWebServerHttps	HTTPS	443	No	
RMIClassLoader	RMI	51099	No	
RMIClassLoaderHttps	RMI (SSL)	5443	No	
RMIIFRegist	RMI	1099	No	
PreRMIServer	RMI	51100-51355[1]	No	
		Automatic allocation		83-03-01-xx/00 or later
DKCManPrivate	RMI	11099	N/A	83-01-24-xx/00 or later
SMI-S (SLP)	SLP	427	Yes, only if SMI-S is not used.	
SMIS_CIMOM	SMI-S	5989-6244[1]	Yes, only if SMI-S is not used.	83-01-20-xx/00 or later
		Automatic allocation		83-03-01-xx/00 or later
CommonJettyStart	HTTP	8080	N/A	83-01-24-xx/00 or later
CommonJettyStop	HTTP	8210	N/A	
RestAPIServerStop	HTTP	9210	N/A	

Port number key name (Windows Firewall Inbound name)	Protocol	Initial value of port number	Can the port be closed?	SVP software version
DeviceJettyStart	HTTP	8081	N/A	
		Automatic allocation		83-03-01-xx/00 or later
DeviceJettyStop	HTTP	8211	N/A	83-01-24-xx/00 or later
		Automatic allocation		83-03-01-xx/00 or later
Hi-Track	HTTPS, FTP (SSL)	4431	Yes, only if Hi-Track is not used.	83-04-00-xx/00 or later

Note:

1. When the SVP software version is 83-03-01-xx/00 or later, unused port numbers are allocated automatically from the described range during storage system registration and a firewall is also set. The allocated ports numbers are used when starting the storage system. When the SVP software version is earlier than 83-03-01-xx/00, ports 51100 and 5989 are used respectively.

The following TCP/IP port assignments are used by the storage system, other devices, and applications.

Port number	Usage description
80	Used by the SVP, Hitachi Storage Advisor, and Device Manager - Storage Navigatorto communicate through the HTTP protocol.
161	UDP (SNMP uses this port to send traps from the storage system) .
427	Used by SMI-S.
1099	Used by Hitachi Command Suite products JAVA RMI Registry server.
2000	TCP (Device Manager - Storage Navigator: Nonsecure) Cisco Skinny Client Control Protocol (SCCP) uses port 2000 for TCP. If you use Device Manager - Storage Navigator in a network with SCCP, change the TCP port that Device Manager - Storage Navigator uses (refer to the Device Manager - Storage Navigator online help).
5989	Used by SMI-S.
10995	TCP Device Manager - Storage Navigator and Hitachi suite components)
23015	Used for Web browser communications.
23016	Used for Web browser communications via SSL.
28355	TCP (Device Manager - Storage Navigator: Secure)
31001	Used for communication by Hitachi Command Control Interface (CCI) data collection procedures.
34001	Used by RAID Manager.
51099	Used by Device Manager - Storage Navigator for communication.
51100	Used by Device Manager - Storage Navigator for communication.

- The effective range of the port number is 0 to 65535. Select a number that is not already in use by another service.
- Do not use port numbers from 1 to 1023 because they are reserved in other applications. Instead, change the port numbers to 1024 or higher. However, the port numbers of 2049, 4045, and 6000 cannot be used for MAPPWebServer and MAPPWebServerHttps.

- Multiple command input parameters "`[Port Number Key] _ [Port Number]`" can be specified. The _ character indicates a space. For example:

  ```
  MappSetPortEdit.bat MAPPWebServer 81 MAPPWebServerHttps 444
  ```

- A management file of the port numbers used in the SVP follows. For example: The management file of the port numbers is for reference only and should not be changed. Close the management file of the port numbers when issuing the change (initialization) command.

  ```
  <The directory where the tool exists>\mpprt\cn
  \mappsetportset.properties
  ```

  ```
  C:\Mapp\wk\Supervisor\mappiniset\mpprt\cnf
  \mappsetportset.properties
  ```

- Verify the port numbers to be used in the SVP. See Viewing the port number to be used in the SVP (on page 140) .
- The completion message is displayed following the service restart message.
- The port number key name is case sensitive.

5. A service restart message appears followed by a completion message.
6. At the message `Press any key to continue`, press any key to continue.
7. Exit from the command prompt.

Initializing SVP port numbers

You can reset SVP port numbers to their initial setting. Resetting the port numbers restarts the SVP. To initialize the automatically allocated port numbers, see Initializing automatically allocated port numbers (on page 137) .

Before you begin

- Connect the management console PC to the SVP.
- Verify the client PC is already connected to the SVP using Remote Desktop Connection.
- Verify that you are logged out of HDvM - SN.

Procedure

1. On the SVP, exit to a Windows command prompt as Administrator.

2. Change to the directory where the tool `MappSetPortEdit.bat` is located, and then issue the following command: `C:\Mapp\wk\Supervisor\MappIniSet\MappSetPortEdit.bat`

   > **Tip:** In this command, `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with the appropriate installation directory.

   A confirmation message appears.

3. Enter `y` and press **Enter**.
   A service restart message appears followed by a completion message.
4. At the message `Press any key to continue`, press any key to continue.
5. Exit from the command prompt.

Behavior when changing SVP port numbers

If you change an SVP port number, observe the following considerations.

Port number key name	Effect
MAPPWebServer	**Using Hitachi Device Manager - Storage Navigator** The URL specification method to log on to Storage Navigator changes.
	Using Hitachi Command Suite Match the port number used in Hitachi Command Suite to <SVP Change Port>.
MAPPWebServerHttps	**Using Hitachi Device Manager - Storage Navigator**: None
	Using Hitachi Command Suite Match the port number used in Hitachi Command Suite to <SVP Change Port>.
RMIClassLoader	None
RMIClassLoader	**Using Hitachi Command Suite** Match the port number used in Hitachi Command Suite to <SVP Change Port>.

RMIClassLoaderHttps	Using **Hitachi Device Manager - Storage Navigator** When using the `raidinf` command (a program for obtaining configuration reports and obtaining tier relocation logs) to log on to Device Manager - Storage Navigator, specify <SVP Change Port> in addition to the SVP IP address or host name.
RMIIFRegist	When issuing the remote power ON/OFF tool (RmtPsTool) command, specify <SVP Change Port> for the Management Server Port Number parameter.
	When issuing the export tool command, specify <SVP Change Port> in addition to the SVP IP address using `ip Subcommand` to the SVP IP address.
	Using Hitachi Command Suite Match the port number used in Hitachi Command Suite to the new SVP port.
PreRMIServer	None
DKCManPrivate	None
SMI-S (SLP)	**Using SMI-S:** Match the port number used in the SMI-S communication to <SVP Change Port>.
SMIS_CIMOM	Match the port number used in the SMI-S communication to <SVP Change Port>. For a storage system running firmware version 83-03-01-xx/00 or later, register the storage system, and then set it after verifying the port numbers to be used (see Viewing the port number to be used in the SVP (on page 140))
CommonJettyStart	None
CommonJettyStop	None
RestAPIServerStop	None
DeviceJettyStart	None
DeviceJettyStop	None

Reallocating automatically allocated port numbers

You can reassign the port numbers automatically allocated to the storage system. When the port numbers assigned to the storage system are used in other applications, the port numbers are reallocated to the ports.

Note:

- Stop the service of the storage system to be reallocated, and then perform reallocation. If the service is performed without stopping it, stop the service of the target storage system in the **Storage Device List** window, and then start the service.
- The DeviceJettyStart and DeviceJettyStop ports that are allocated when the storage system service is started are not reallocated.
- When the function using the ports is disabled, delete the allocated port numbers.

Procedure

1. Log out of Hitachi Device Manager - Storage Navigator from the storage system to be reallocated.
2. Stop the service of the storage system.
3. On the SVP, start a Windows command prompt as an Administrator.
4. Change the current directory to the directory where the tool exists. Run the following command: `C:\Mapp\wk\Supervisor\MappIniSet \MappPortManageRenum.bat_[Serial number](arbitrary)`

   The _ character indicates a space. The values in [ ] indicates a parameter.

   When the `[Serial number]` is omitted, the command is performed for storage systems running firmware version 83-03-01-xx/00 or later.

   Tip: In this command, `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\MAPP`, replace `C:\MAPP` with the appropriate installation directory.
5. The confirmation message for reallocation is displayed. To continue the processing, enter `y`, and then press **Enter**. To cancel the processing, enter `n`, and then press **Enter**.
6. Close the command prompt.
7. Start the services of the reallocated storage system.

Initializing automatically allocated port numbers

Before you begin

- Verify the client PC is already connected to the SVP through the Remote Desktop Connection.
- Stop the services of all the storage systems that have a Ready status in the **Storage Device List** window, and then initialize them.
- If storage systems are initialized without stopping the services, the storage system port numbers get reallocated automatically. For more information, see Reallocating automatically allocated port numbers (on page 136) .

Procedure

1. Log out of Device Manager - Storage Navigator.
2. In the **Storage Device List** window, stop the services of all the storage systems that have a **Ready** status.
3. On the SVP, start a Windows command prompt as an Administrator.
4. Change the current directory to the directory where the tool exists and run the following command: `C:\Mapp\wk\Supervisor\MappIniSet\MappPortManageInit.bat`

   > **Tip:** `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with the appropriate installation directory.

5. At the confirmation message for reallocation, enter `y` and press **Enter** to continue or enter `n` and press **Enter** to cancel the processing.
6. At the completion message, press any key to continue.
7. Perform the reallocation by running the following command: `C:\Mapp\wk\Supervisor\MappIniSet\MappPortManageRenum.bat_[Serial number] (arbitrary)`

   If the `[Serial number]` is omitted, the command is performed for storage systems running firmware version 83-03-01-xx/00 or later.

   > **Tip:** `C:\MAPP` indicates the installation directory of the storage management software and SVP software. When the installation directory, other than `C:\Mapp` is specified, replace `C:\MAPP` with the specified installation directory.

8. At the confirmation message for reallocation, type `y` and press **Enter** to continue or type `n` and press **Enter** to cancel the processing.
9. At the completion message, press any key to continue.
10. Repeat steps 6 through 9 to reallocate the port numbers for all the registered storage systems.
11. Close the command prompt.

12. Start the service of the storage system.

Changing range of port numbers to be allocated automatically

Before you begin

Verify that the client PC is already connected to the SVP through the Remote Desktop Connection.

Procedure

1. On the SVP, start a Windows command prompt as an Administrator.
2. Change the current directory to the directory where the tool exists and run the following command: `C:\Mapp\wk\Supervisor\MappIniSet>MappPortRangeSet.batr[Service port number]_[Range of port numbers]`

   > **Tip:** `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with the appropriate installation directory.

Note:

Port number key name and **Default value of port number range** can be changed as shown in the following table. Zero number port is not allocated regardless of this command setting.

Port Number Key Name	Default value of port number range	Comments
PreRMIServer	51100 to 51355	-
SMIS_CIMOM	5989 to 6244	-
DeviceJettyStart	48081 to 48336	-
DeviceJettyStop	48411 to 48666	-
N/A	1 to 1023	Port numbers that are not used by automatic allocation

- The effective range of the port number range is 1 to 65535. Set the port numbers so as to avoid conflict with those used in other services.
- Port numbers 1 to 1023 are reserved in other applications. If 1 to 1023 are excluded from the unavailable setting value, the applications might not operate normally.
- The available character strings in the effective range are as follows:

  "Number" "," "-" "rm"

  If "rm" is specified, delete the setting of the specified port number key.
- You can specify more than one command input parameter “[Service port number key name] * [Port number range] where ***** is a one-byte space.

  For example, `MappPortRangeSet.bat PreRMIServer 51200-55000 SMIS_CIMOM 5989-6244,8000`
- The port number range set for unavailable cannot be used, even if it is an effective range for other keys.

  For example, when PreRMIServer 51100-51355 unavailable 51100-51200 is set, the port number range allocated by PreRMIServer is 51201 to 51355.

3. A completion message appears. Press any key to continue.
4. Close the command prompt.

Initializing range of port numbers to be allocated automatically

You can initialize the range of the port numbers automatically allocated to the storage system.

Before you begin

Verify the client PC is already connected to the SVP through a Remote Desktop connection.

Procedure

1. On the SVP, start a Windows command prompt as an Administrator.
2. Change the current directory to the directory where the tool exists and run the following command: `C:\Mapp\wk\Supervisor\MappIniSet\MappPortRangeInit.bat`

   > **Tip:** `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with the appropriate installation directory.

3. The confirmation message for reallocation is displayed. To continue the processing, enter `y`, and then press **Enter**. To cancel the processing, enter `n`, and then press **Enter**.
   A completion message appears. Press any key to continue.
4. Close the command prompt.

Viewing the port number to be used in the SVP

You can view the port numbers to be used in the SVP.

Before you begin

Verify the client PC is already connected to the SVP through the Remote Desktop connection.

Procedure

1. On the SVP, start a Windows command prompt as an Administrator.
2. Change the current directory to the directory where the tool exists and run the following command: `C:\Mapp\wk\Supervisor\MappIniSet\MappPortRefer.bat_[Serial number] (arbitrary)`

   The _ character indicates a space. The values in [ ] indicates a parameter.

   When the serial numbers are omitted, the information of all the storage systems registered in Storage Device List is displayed.

> **Tip:** `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with the appropriate installation directory.

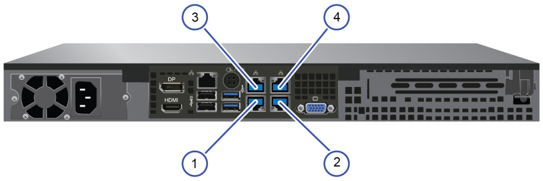
3. The information of the port numbers to be used in the SVP is displayed. For the ports whose numbers are not allocated, **Not Defined** is displayed.
4. A completion message appears. Press any key to continue.
5. Close the command prompt.

Chapter 15: Editing the Storage Device List

If you change the storage system IP address or the maintenance password, edit the Storage Device List to reflect the change.

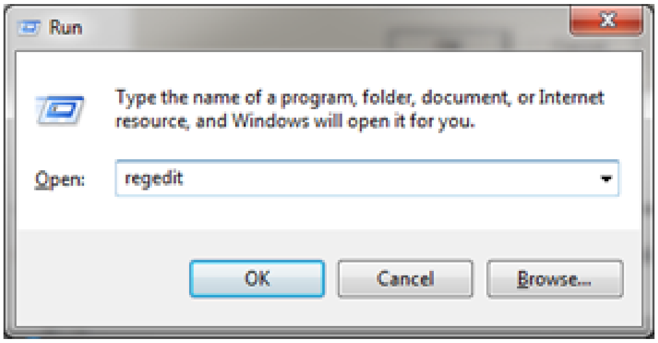
Procedure

1. If your network uses the spanning tree protocol (STP) Bridge Protocol Data Unit (BPDU) guard on your network, perform the following Registry changes. Otherwise, skip to step 2:
   a. If you use the physical SVP supplied by Hitachi Vantara, verify the following connections.



SVP LAN Port	Description
1	Do not connect a cable to the LAN 1 port at this time. You will connect to this port after you complete the **Initial Startup** wizard.
2	Connect the LAN 2 port to a Windows-based management console.
3	The LAN 3 port is already connected to the user LAN port on controller 1.
4	The LAN 4 port is already connected to the user LAN port on controller 2.

   b. If you use the physical SVP supplied by Hitachi Vantara, remove the cable from the **LAN1** port on the SVP.
   c. Click **Start** > **Run**.
   d. In the **Run** dialog box, type `regedit`, and then click **OK**.

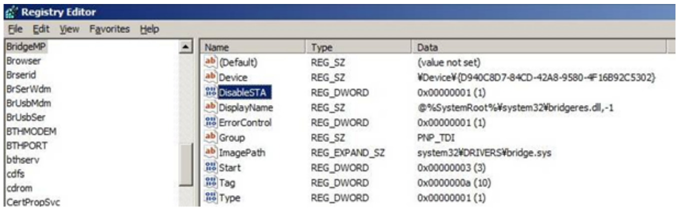


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

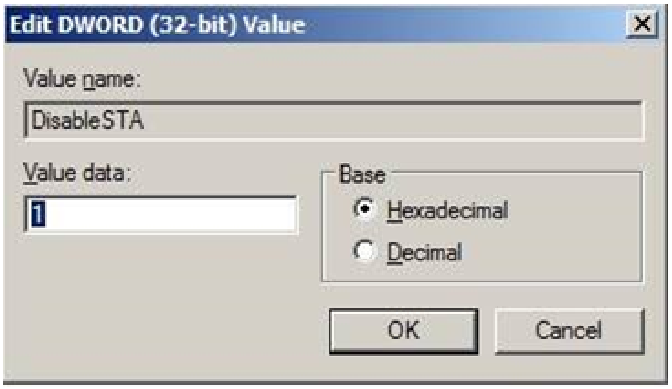
e. Go to the following key: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BridgeMP`

f. Right-click **New** > **DWORD (32-bit Value)**, and then type `DisableSTA`.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Device	REG_SZ	¥Device¥{D940C8D7-84CD-42A8-9580-4F16B92C5302}
DisableSTA	REG_DWORD	0x00000001 (1)
DisplayName	REG_SZ	@%SystemRoot%¥system32¥bridgeres.dll,-1
ErrorControl	REG_DWORD	0x00000001 (1)
Group	REG_SZ	PNP_TDI
ImagePath	REG_EXPAND_SZ	system32¥DRIVERS¥bridge.sys
Start	REG_DWORD	0x00000003 (3)
Tag	REG_DWORD	0x0000000a (10)
Type	REG_DWORD	0x00000001 (1)

g. For the `DisableSTA` DWORD, change the hexadecimal **Value data** value to `1`, and then click **OK**.



Value name: DisableSTA

Value data: 1

Base

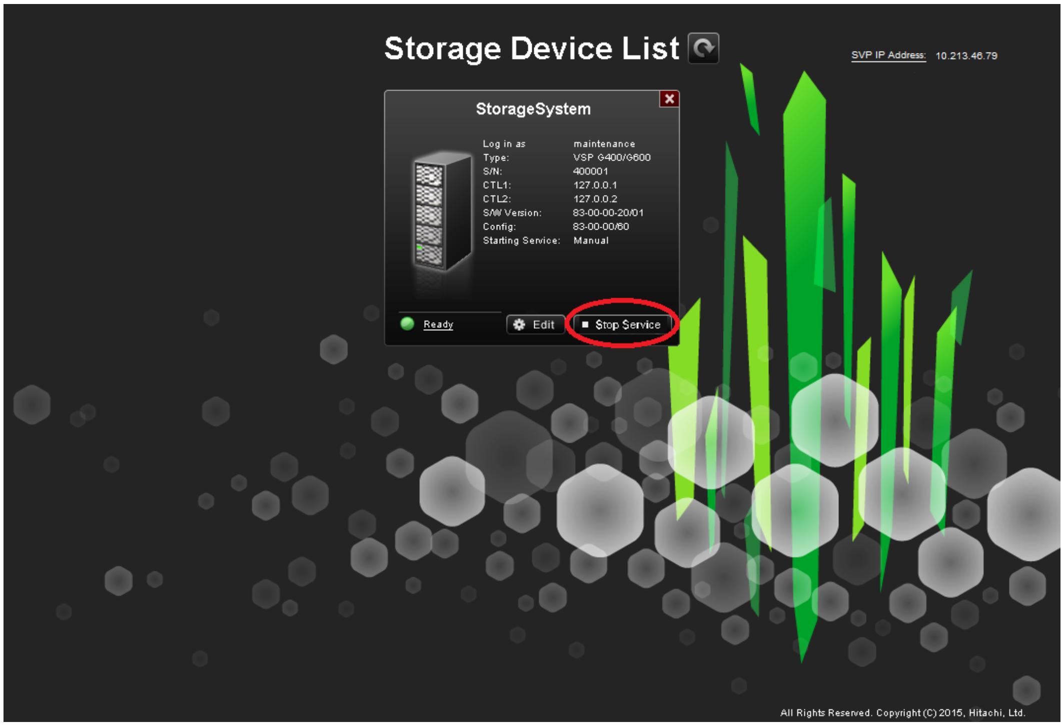
● Hexadecimal

○ Decimal

h. Restart the SVP, reconnect the cable to the **LAN1** port on the SVP, and verify connectivity through the network to the SVP.

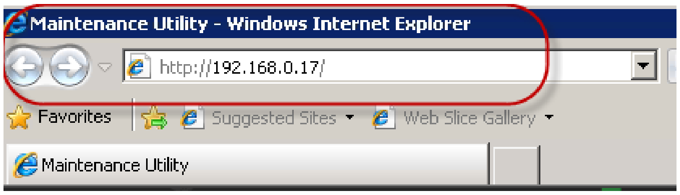
2. Using Remote Desktop Connection, access the SVP using the storage system's maintenance LAN port of `10.0.0.100`.

3. In the **Storage Device List** window, click **Stop Service**. Wait up to five minutes for the service to stop.

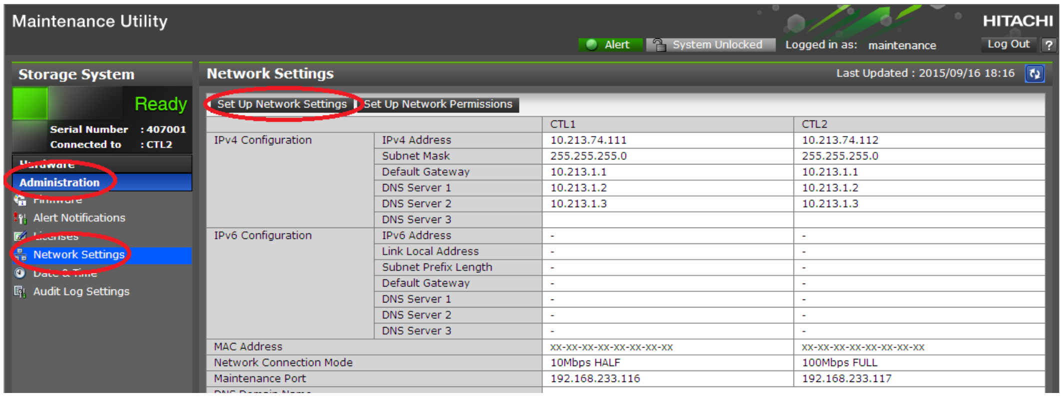

Storage Device List
SVP IP Address: 10.213.46.79
StorageSystem
Ready
Edit
Stop Service
All Rights Reserved. Copyright (C) 2015, Hitachi, Ltd.

Log in as maintenance
Type: VSP G400/G600
S/N: 400001
CTL1: 127.0.0.1
CTL2: 127.0.0.2
S/W Version: 83-00-00-20/01
Config: 83-00-00/60
Starting Service: Manual

4. Log on to the maintenance utility.



5. In the maintenance utility, click **Administration** > **Network Setting**, and then click **Set Up Network Settings**.



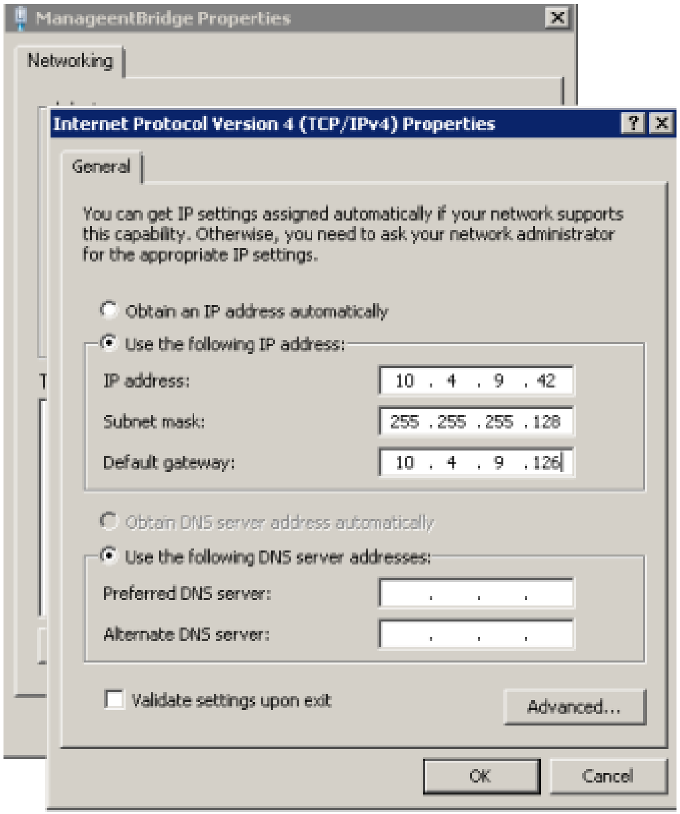
Logged in as: maintenance

Serial Number : 407001
Connected to : CTL2

Last Updated : 2015/09/16 18:16

		CTL1	CTL2
IPv4 Configuration	IPv4 Address	10.213.74.111	10.213.74.112
	Subnet Mask	255.255.255.0	255.255.255.0
	Default Gateway	10.213.1.1	10.213.1.1
	DNS Server 1	10.213.1.2	10.213.1.2
	DNS Server 2	10.213.1.3	10.213.1.3
	DNS Server 3		
IPv6 Configuration	IPv6 Address	-	-
	Link Local Address	-	-
	Subnet Prefix Length	-	-
	Default Gateway	-	-
	DNS Server 1	-	-
	DNS Server 2	-	-
	DNS Server 3	-	-
MAC Address		xx-xx-xx-xx-xx-xx-xx-xx	xx-xx-xx-xx-xx-xx-xx-xx
Network Connection Mode		10Mbps HALF	100Mbps FULL
Maintenance Port		192.168.233.116	192.168.233.117

6. Change the CTL1 and CTL2 LAN IP addresses, as required.
7. Change the properties of the network bridge to reflect your IP address, subnet, and default gateway settings.



ManageentBridge Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Advanced...
OK
Cancel

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 4 . 9 . 42

Subnet mask: 255 . 255 . 255 . 128

Default gateway: 10 . 4 . 9 . 126

○ Obtain DNS server address automatically

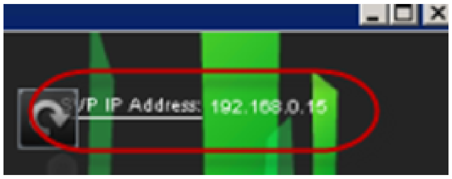
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

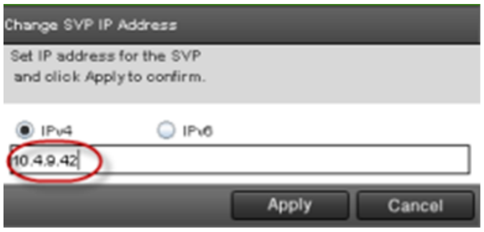
□ Validate settings upon exit

8. To verify that the new LAN IP settings are correct for your environment, exit to a command prompt (DOS) window and ping controller 1 and controller 2 using the new IP addresses. Do not proceed until this step is successful.
9. In the **Storage Device List** window, click the SVP IP address setting in the top-right of the window.



SVP IP Address: 192.168.0.15

10. Change the SVP IP address to match the new bridge IP address setting, and then click **Apply**.

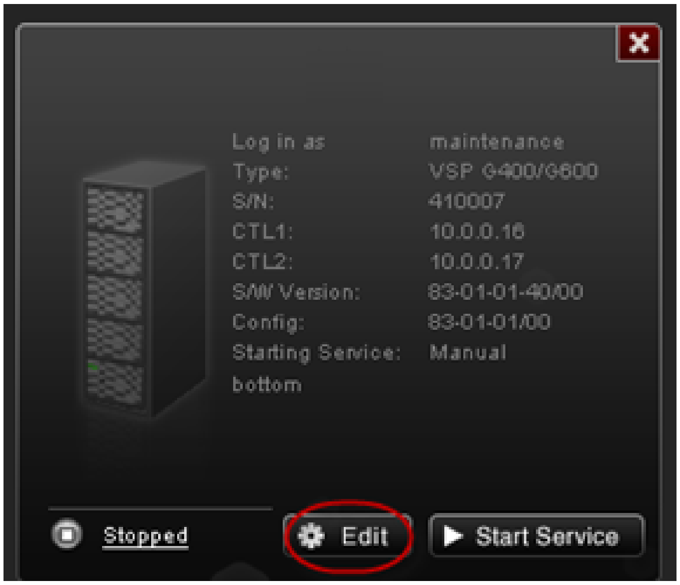


Set IP address for the SVP and click Apply to confirm.

● IPv4 ○ IPv6

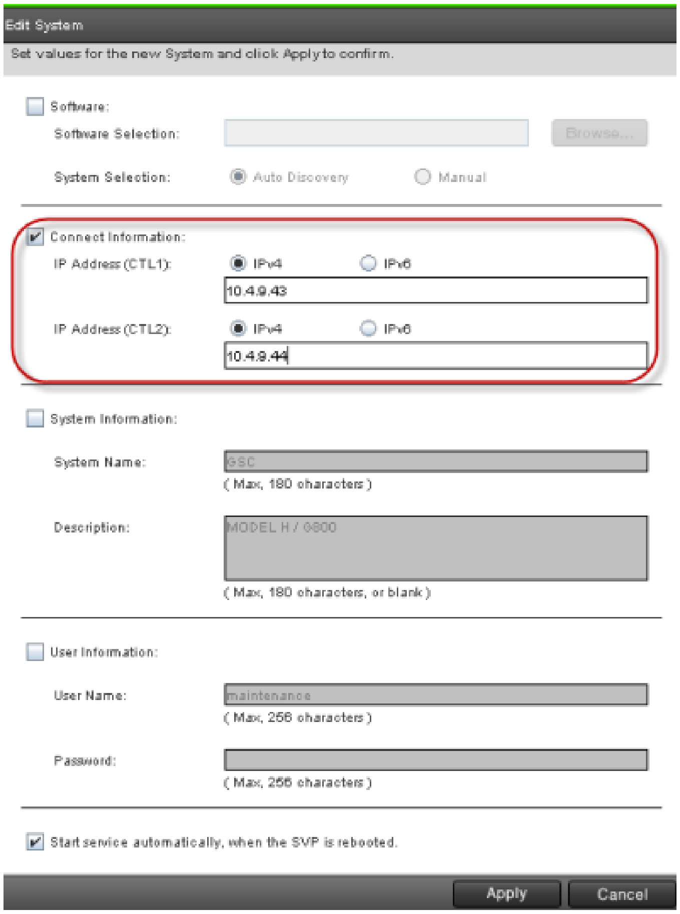
10.4.9.42

11. In the **Storage Device List** window, click **Edit**.



Log in as	maintenance
Type:	VSP G400/G600
S/N:	410007
CTL1:	10.0.0.16
CTL2:	10.0.0.17
S/W Version:	83-01-01-40/00
Config:	83-01-01/00
Starting Service:	Manual
bottom	

12. Select the **Connect Information** check box, change the IP addresses for **CTL1** and **CTL2**, and then click **Apply**.



Edit System

Set values for the new System and click Apply to confirm.

□ Software:

Software Selection: Browse...

System Selection: ● Auto Discovery ○ Manual

☑ Connect Information:

IP Address (CTL1): ● IPv4 ○ IPv6

10.4.9.43

IP Address (CTL2): ● IPv4 ○ IPv6

10.4.9.44

□ System Information:

System Name: GSC

(Max. 180 characters)

Description: MODEL H / G800

(Max. 180 characters, or blank)

□ User Information:

User Name: maintenance

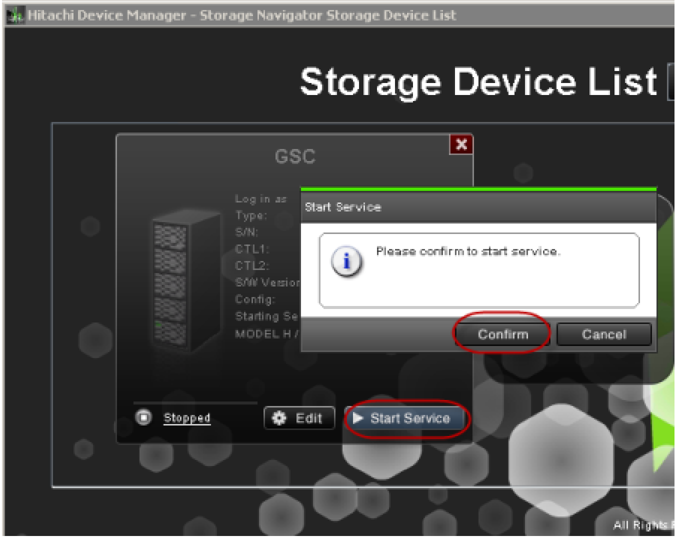
(Max. 256 characters)

Password:

(Max. 256 characters)

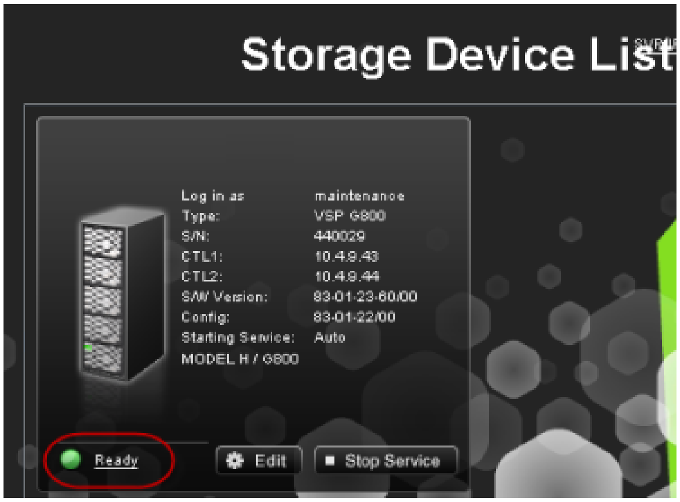
☑ Start service automatically, when the SVP is rebooted.

13. In the **Storage Device List** window, click **Start Service**. At the confirmation message, click **Confirm**.



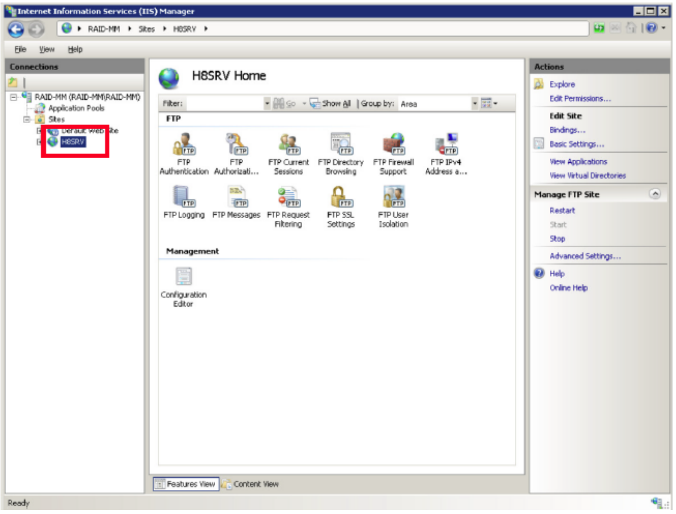
Please confirm to start service.

14. Using Remote Desktop Connection, access the SVP using the new user LAN IP address.
15. Open the **Storage Device List** window and verify that services are ready.

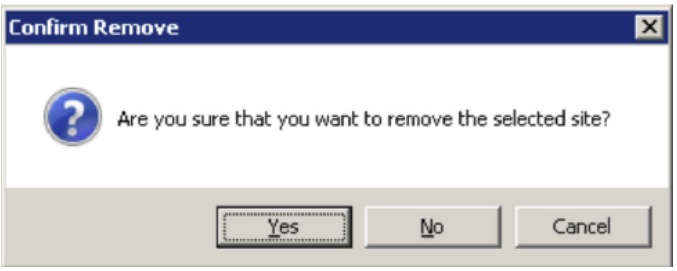


Log in as	maintenance
Type:	VSP G800
S/N:	440029
CTL1:	10.4.9.43
CTL2:	10.4.9.44
S/W Version:	83-01-23-60/00
Config:	83-01-22/00
Starting Service:	Auto
MODEL H / G800	

16. Verify information internet service (IIS) FTP settings.
    a. Using a maintenance PC, from the Control Panel, open **Administrative Tools** and start **Internet Information Services (IIS) Manager**.
    b. If the default website and the existing FTP server (including H8SRV) are registered, right-click the FTP server under **Sites**, and then click **Delete**.

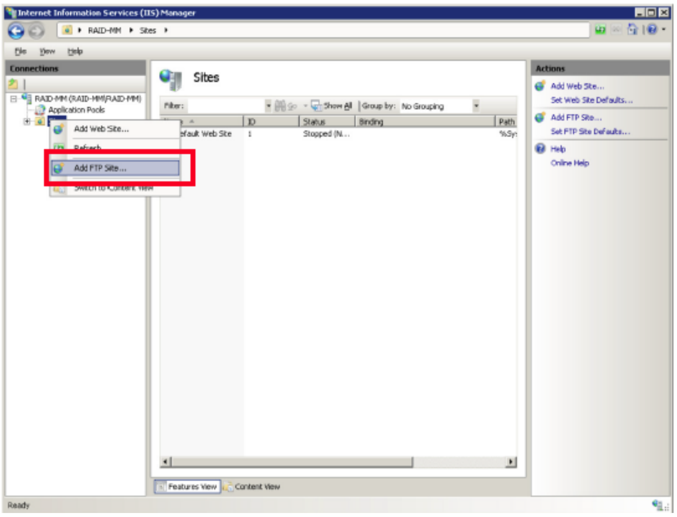


At the **Confirm Remove** message, click **Yes**. Repeat this step for the default website and other FTP servers.



Are you sure that you want to remove the selected site?

c. Right-click **Sites**, and then click **Add FTP Site**.

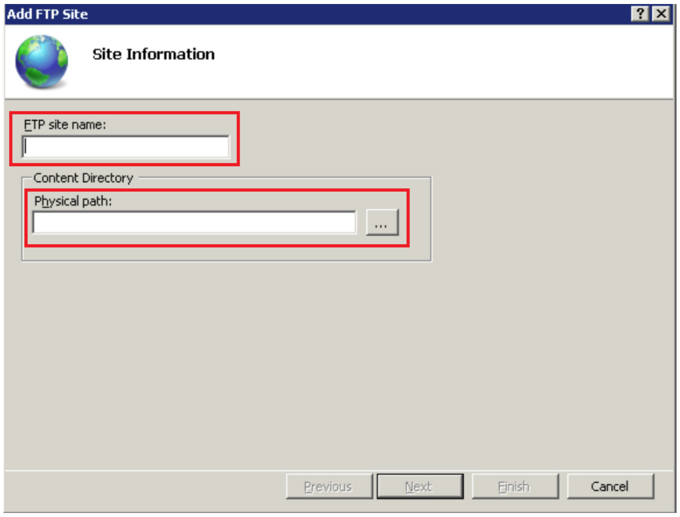


d. For **FTP site name**, type `H8SRV`. For **Content Directory**, type `C:\Mapp\wk\83xxxxyyyyyy\DKC200\HOME\micro`. Click **Next**.

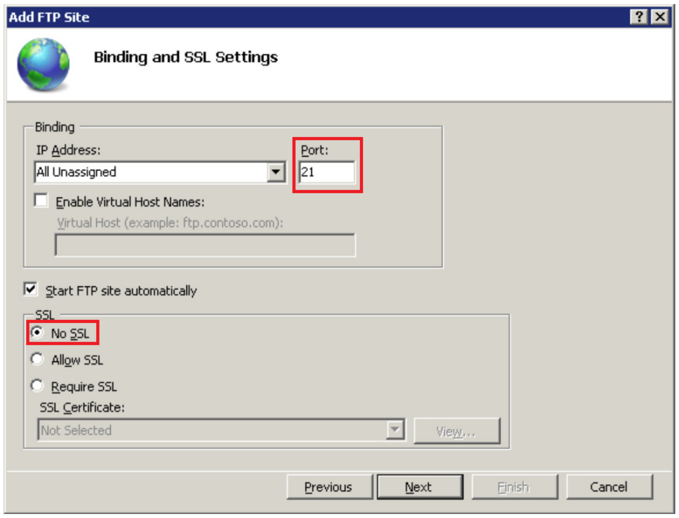
The `83xxxxyyyyyy` directory is created when the following storage systems are registered in the **Storage Device List** window:

- `6000`: VSP G800 or VSP F800
- `4000`: VSP G400, G600 or VSP F400, F600

- `2000`: VSP G200
- `yyyyyy` = serial number



e. For **Port**, type `21`. For **SSL**, click **No SSL**. Click **Next**.



IP Address: All Unassigned

Port: 21

□ Enable Virtual Host Names:

Virtual Host (example: ftp.contoso.com):

☑ Start FTP site automatically

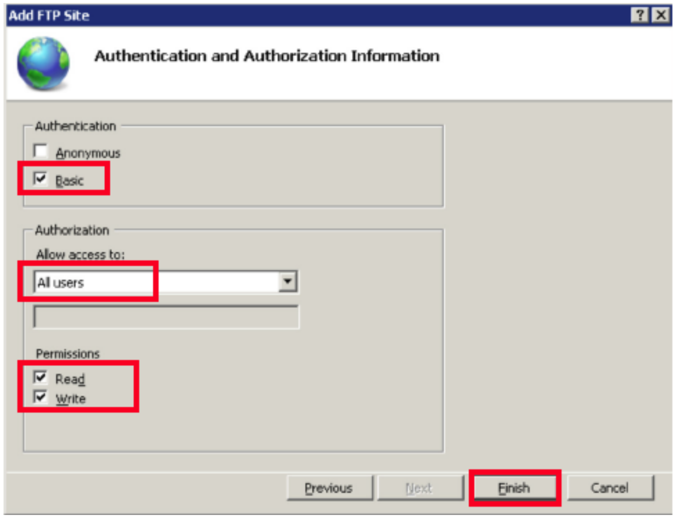
● No SSL

○ Allow SSL

○ Require SSL

SSL Certificate: Not Selected

f. For **Authentication**, select **Basic**. For **Authorization**, select **All users**. For **Permissions**, select **Read** and **Write**. Click **Finish**.



Authentication

☐ Anonymous

☑ Basic

Authorization

Allow access to:

All users

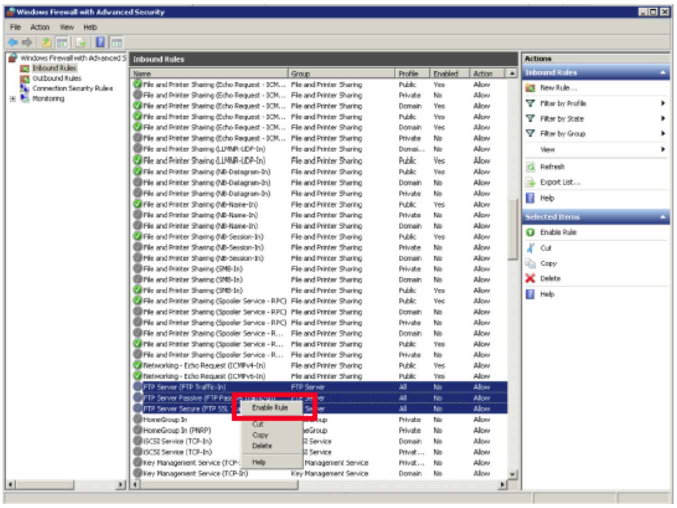
Permissions

☑ Read

☑ Write

g. From the Control Panel, open **Administrative Tools** and start **Windows Firewall with Advanced Security**.

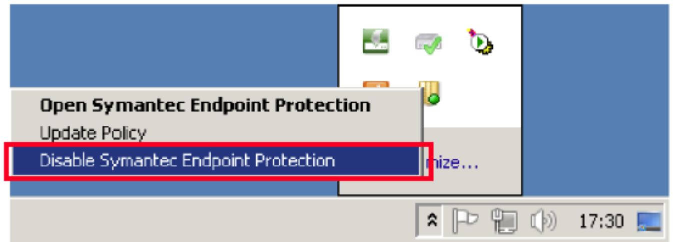
h. In the tree in the left pane, click **Inbound Rules**, and then click **FTP Server Passive**, **FTP Server Secure**, and **FTP Server**. Right-click, and then click **Enable Rule**.



Inbound Rules

Name	Group	Profile	Enabled	Action
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Private	No	Allow
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Domain	Yes	Allow
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Domain	Yes	Allow
File and Printer Sharing (Echo Request - ICM...	File and Printer Sharing	Private	No	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Domai...	No	Allow
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private	No	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private	No	Allow
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private	No	Allow
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private	No	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (SMB-In)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Private	No	Allow
File and Printer Sharing (Spooler Service - R...	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (Spooler Service - R...	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Spooler Service - R...	File and Printer Sharing	Private	No	Allow
Networking - Echo Request (ICMPv4-In)	File and Printer Sharing	Public	Yes	Allow
Networking - Echo Request (ICMPv6-In)	File and Printer Sharing	Public	Yes	Allow
FTP Server (FTP Traffic-In)	FTP Server	All	No	Allow
FTP Server Passive (FTP Pas	Server	All	No	Allow
FTP Server Secure (FTP SSL	Server	All	No	Allow
HomeGroup In	oup	Private	No	Allow
HomeGroup In (PNRP)	eGroup	Private	No	Allow
iSCSI Service (TCP-In)	I Service	Domain	No	Allow
iSCSI Service (TCP-In)	I Service	Privat...	No	Allow
Key Management Service (TCP-	Management Service	Privat...	No	Allow
Key Management Service (TCP-In)	Key Management Service	Domain	No	Allow

i. If you use FTP (IIS), disable the security software. For Symantec Endpoint Protection, for example, right-click the **Symantec Endpoint Protection** icon on the desktop, and then click **Disable Symantec Endpoint Protection**.



Open Symantec Endpoint Protection
Update Policy
Disable Symantec Endpoint Protection
nize...
17:30

Chapter 16: Deleting and registering the storage system

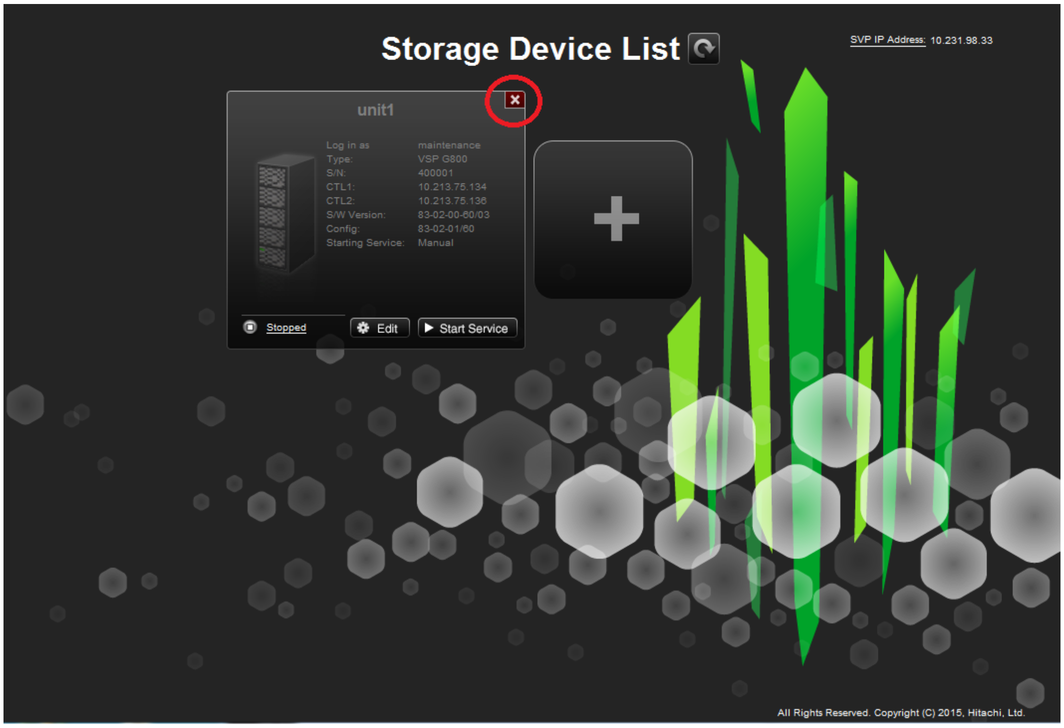
In the unlikely event you need to delete the storage system from the Storage Device List, use the following instructions to delete the storage system, and then register it on the SVP.

Deleting the registered storage system from the Storage Device List

Use the following procedure if you must delete the registered storage system from the **Storage Device List** window.

Procedure

1. Stop the SVP service (see Stopping and restarting the service in each storage system (on page 90)).
2. On the SVP desktop, double-click the **Open StorageDeviceList** icon.
   The **Storage Device List** window opens.
3. In the **Storage Device List** window, click **x** for the storage system that you want to delete.


Storage Device List
SVP IP Address: 10.231.98.33
unit1
Stopped
Edit
Start Service
+
All Rights Reserved. Copyright (C) 2015, Hitachi, Ltd.

Log in as maintenance
Type: VSP G800
S/N: 400001
CTL1: 10.213.75.134
CTL2: 10.213.75.136
S/W Version: 83-02-00-60/03
Config: 83-02-01/60
Starting Service: Manual

Registering the storage system on the SVP

If you delete the registered storage system from the SVP, you can register the storage system.

Before you begin

- Verify the to-be-registered storage system is operating, and the IP addresses of the SVP and the storage system are using the same subnet.
- Upgrade the firmware for the storage system being registered.

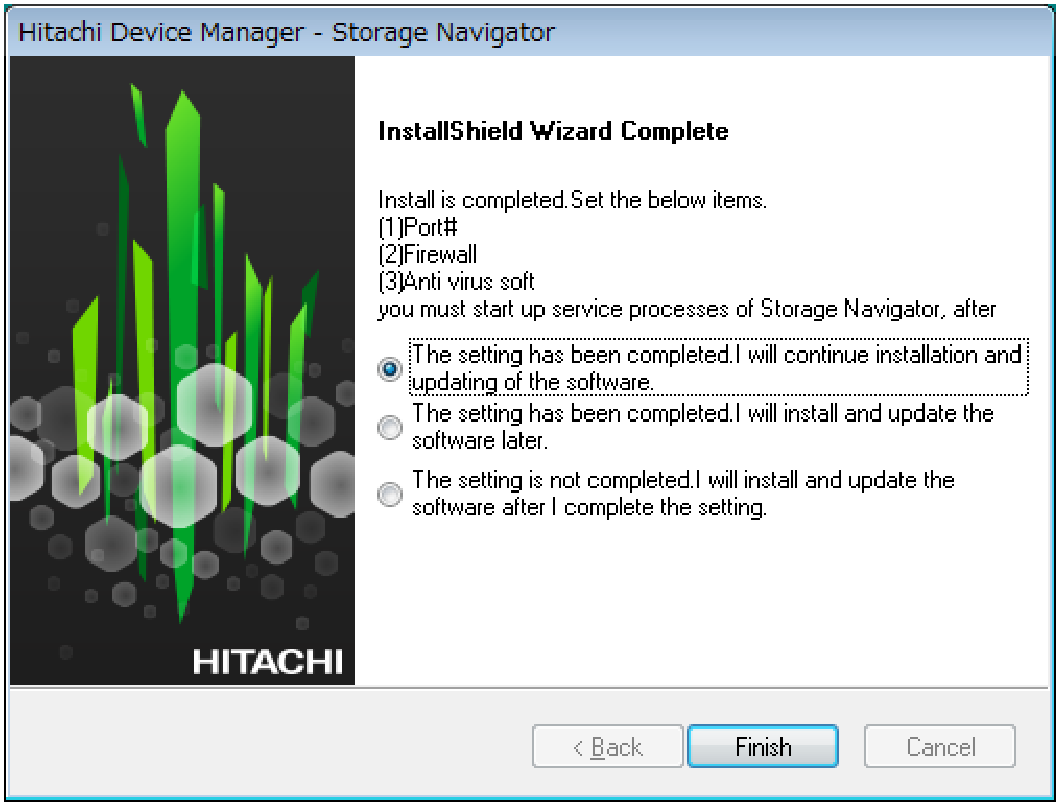
This procedure takes approximately 10 minutes for each storage system to be registered and approximately 200 minutes for each storage system that needs a firmware upgrade.

Note: The upgrade time can take up to 9 hours to complete when NAS modules are installed.

Procedure

1. At the console PC connected to the physical SVP or running the SVP software, insert the media containing the SVP firmware media.
2. On the SVP, create a new folder, and then copy all of the files from the SVP firmware media into the new folder.
3. In the new folder, right-click the `Setup.exe` file and click **Execute as Administrator**.

4. In the following screens, click **Next**, accept the license agreement and click **Next**, and then click **Yes**. If the **Windows Security Alert** window opens, click **Allow access**.
5. Select the top option and then click **Finish**.



Hitachi Device Manager - Storage Navigator

InstallShield Wizard Complete

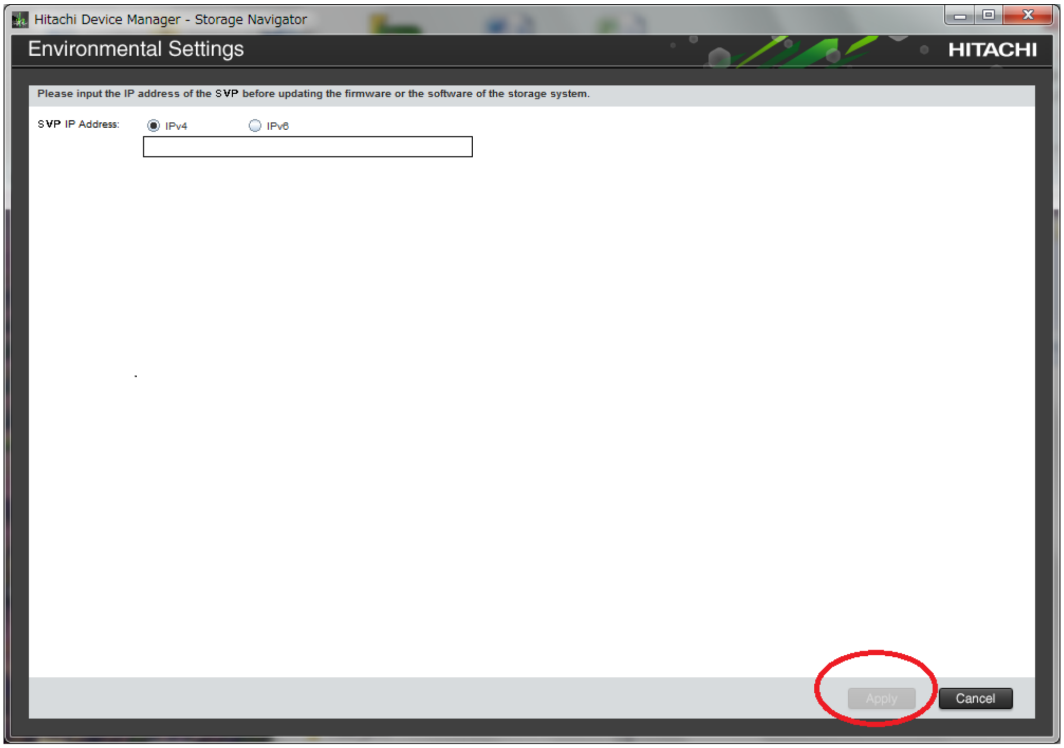
Install is completed.Set the below items.
(1)Port#
(2)Firewall
(3)Anti virus soft
you must start up service processes of Storage Navigator, after

● The setting has been completed.I will continue installation and updating of the software.

○ The setting has been completed.I will install and update the software later.

○ The setting is not completed.I will install and update the software after I complete the setting.

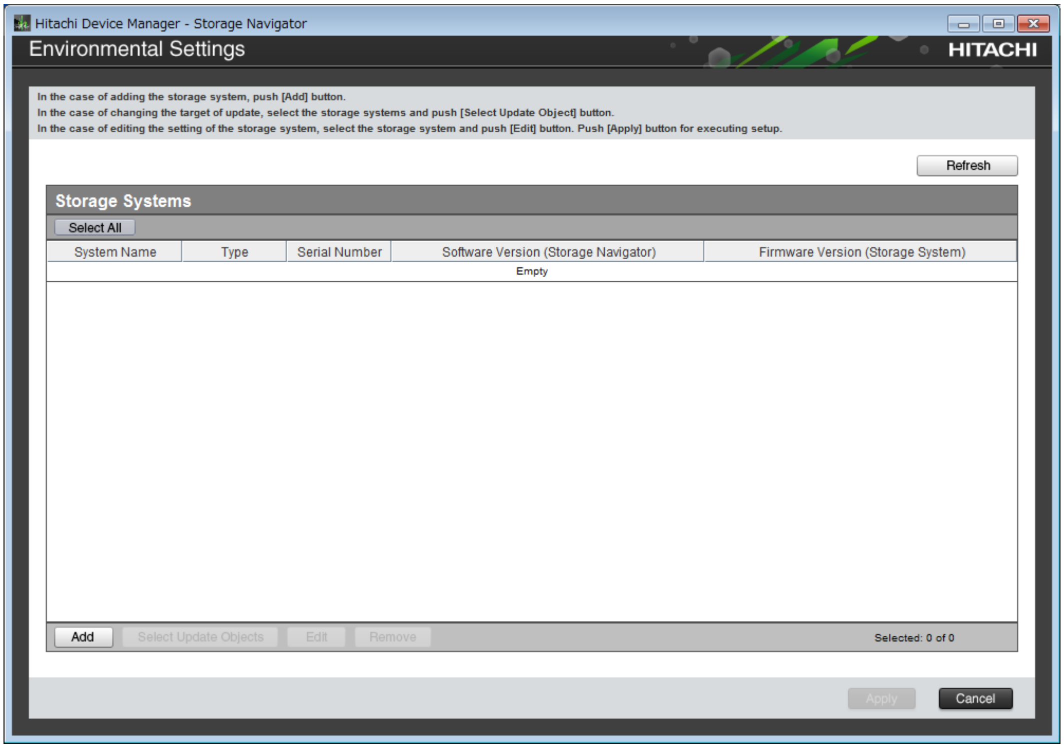
6. When prompted, select the IP addressing method (**IPv4** or **IPv6**), enter the IP address of the port connecting the SVP and the storage system, and then click **Apply**.



Please input the IP address of the SVP before updating the firmware or the software of the storage system.

SVP IP Address: ● IPv4 ○ IPv6

7. When the target storage systems list window opens, click **Add**.

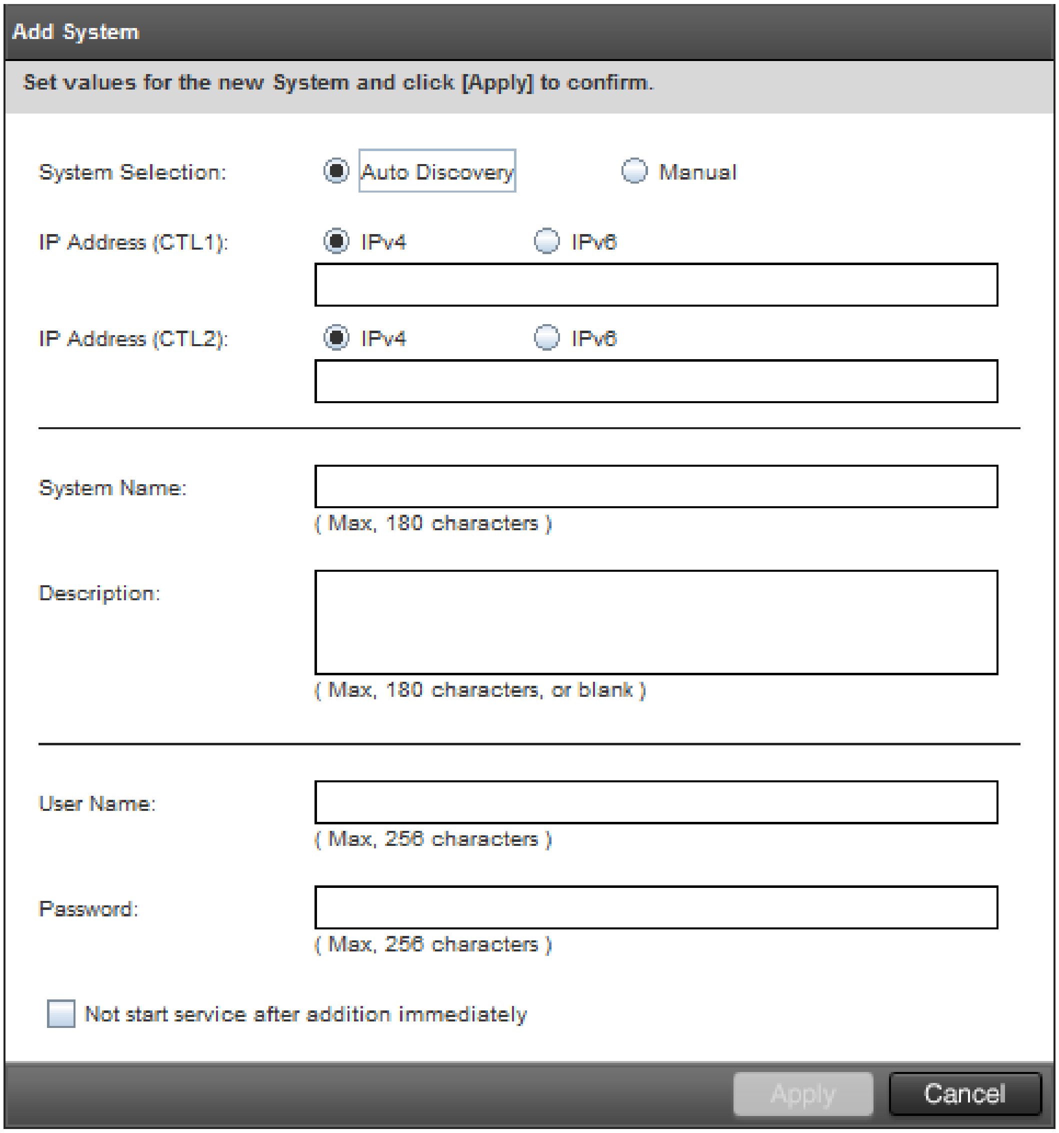


In the case of adding the storage system, push [Add] button.
In the case of changing the target of update, select the storage systems and push [Select Update Object] button.
In the case of editing the setting of the storage system, select the storage system and push [Edit] button. Push [Apply] button for executing setup.

System Name	Type	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
		Empty		

Selected: 0 of 0

The **Add System** window opens.



Add System

Set values for the new System and click [Apply] to confirm.

System Selection: ● Auto Discovery ○ Manual

IP Address (CTL1): ● IPv4 ○ IPv6

IP Address (CTL2): ● IPv4 ○ IPv6

System Name:

(Max, 180 characters)

Description:

(Max, 180 characters, or blank)

User Name:

(Max, 256 characters)

Password:

(Max, 256 characters)

□ Not start service after addition immediately

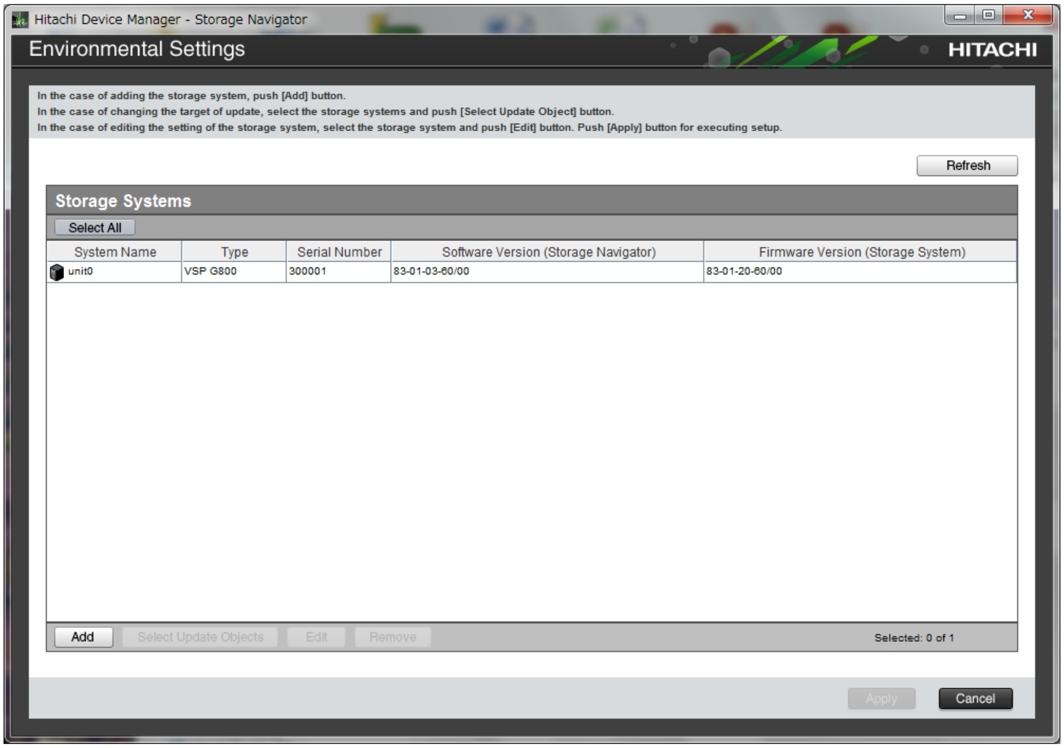
8. In the **Add System** window, complete the fields.

Field	Description
System Selection[1]	Select one of the following methods to discover the storage system. - **Auto Discovery**: Acquire the storage system information automatically. (default) - **Manual**: Specify the storage system manually.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>IP Address (CTL 1)</td><td>Enter the IP address for controller 1. Accept the default <b>IPv4</b> setting or click <b>IPv6</b>, and then enter the IP address in the appropriate format for the addressing method selected.</td></tr>
<tr><td>IP Address (CTL 2)</td><td>Enter the IP address for controller 2. Accept the default <b>IPv4</b> setting or select <b>IPv6</b>, and then click the IP address in the appropriate format for the addressing method selected.</td></tr>
<tr><td>System Name</td><td>Enter the display name of the storage system, up to 180 characters. Permitted characters are one-byte alphanumeric characters and symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~). You cannot use one-byte spaces.</td></tr>
<tr><td>Description</td><td>Enter the description of the storage system, up to 180 characters.</td></tr>
<tr><td>User Name</td><td>Enter a user name. Permitted characters are one-byte alphanumeric characters and symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~). The GUI includes a 256-character limit.</td></tr>
<tr><td>Password</td><td>Enter a password. The GUI includes a 256-character limit.</td></tr>
<tr><td>Do not start service after addition immediately[2]</td><td>Select if you do not want to start service after adding the storage system. (Default is unchecked.)</td></tr>
<tr><td colspan="2"><b>Notes:</b>
1. Service personnel set the storage system information manually. User should not select <b>Manual</b> to set it.
2. To register multiple storage systems, best practice is to check this check box for the settings so that they do not start services while they are added.</td></tr>
</table>

9. Click **Apply**.

The storage system is added to the target storage systems list window.



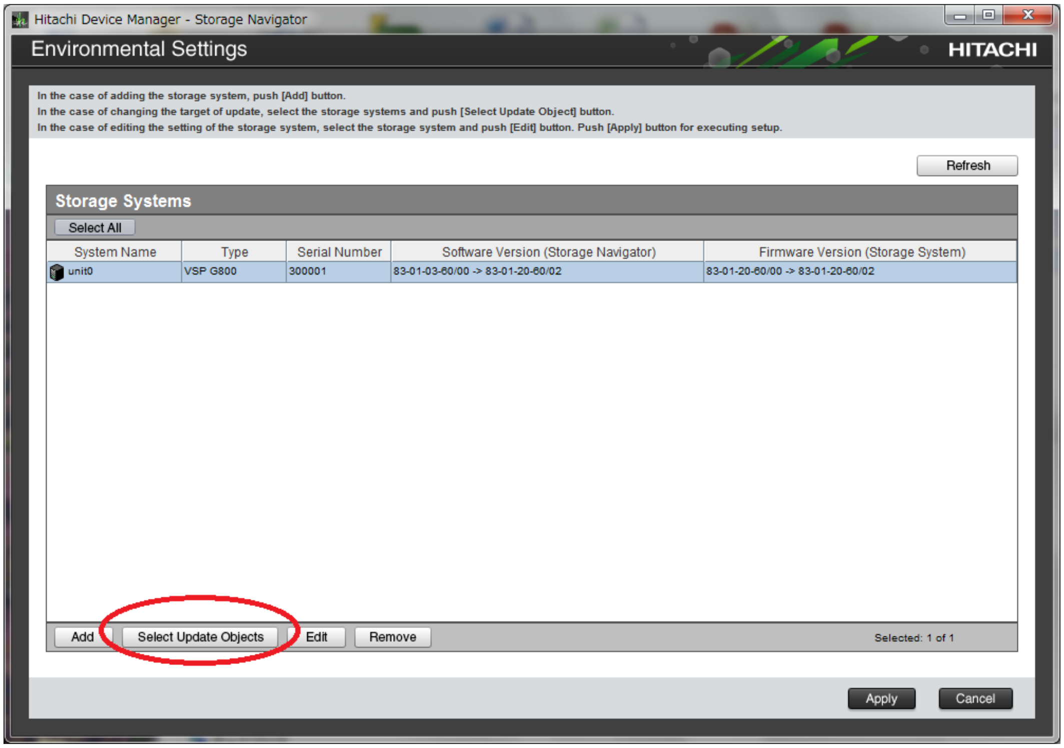
In the case of adding the storage system, push [Add] button.
In the case of changing the target of update, select the storage systems and push [Select Update Object] button.
In the case of editing the setting of the storage system, select the storage system and push [Edit] button. Push [Apply] button for executing setup.

System Name	Type	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
unit0	VSP G800	300001	83-01-03-60/00	83-01-20-60/00

Selected: 0 of 1

Note: If you added the wrong storage system, select the storage system and click **Remove**.

10. To update the firmware and add storage systems at the same time, select the storage systems and click **Select Update Objects**.

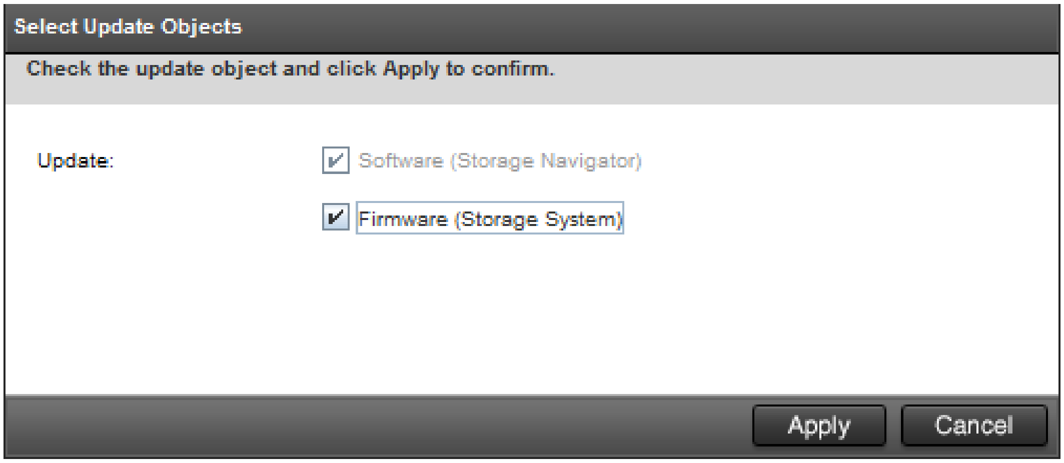


In the case of adding the storage system, push [Add] button.
In the case of changing the target of update, select the storage systems and push [Select Update Object] button.
In the case of editing the setting of the storage system, select the storage system and push [Edit] button. Push [Apply] button for executing setup.

System Name	Type	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
unit0	VSP G800	300001	83-01-03-60/00 -> 83-01-20-60/02	83-01-20-60/00 -> 83-01-20-60/02

Selected: 1 of 1

The **Select Update Objects** window opens.



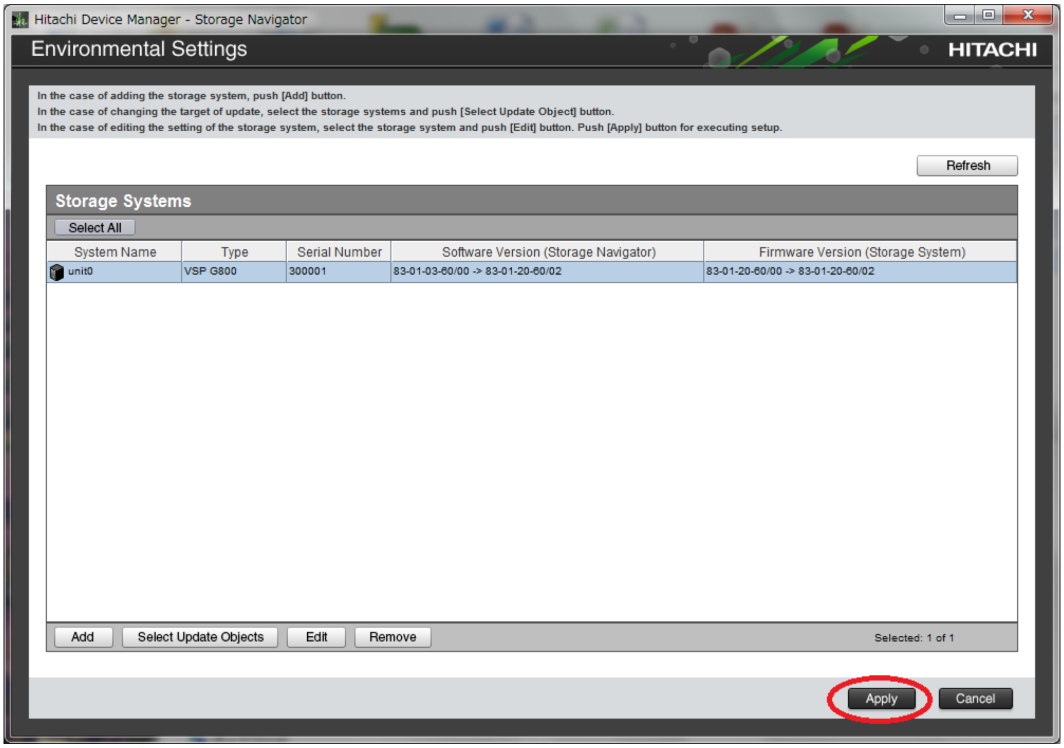
Select Update Objects

Check the update object and click Apply to confirm.

Update: ☑ Software (Storage Navigator)

☑ Firmware (Storage System)

11. To update the firmware of the storage system being registered, check **Firmware (Storage System)**. Otherwise, leave it unchecked.
12. To register additional storage systems, repeat steps 6 through 10.
13. Click **Apply** in the **target storage system** list window.



In the case of adding the storage system, push [Add] button.
In the case of changing the target of update, select the storage systems and push [Select Update Object] button.
In the case of editing the setting of the storage system, select the storage system and push [Edit] button. Push [Apply] button for executing setup.

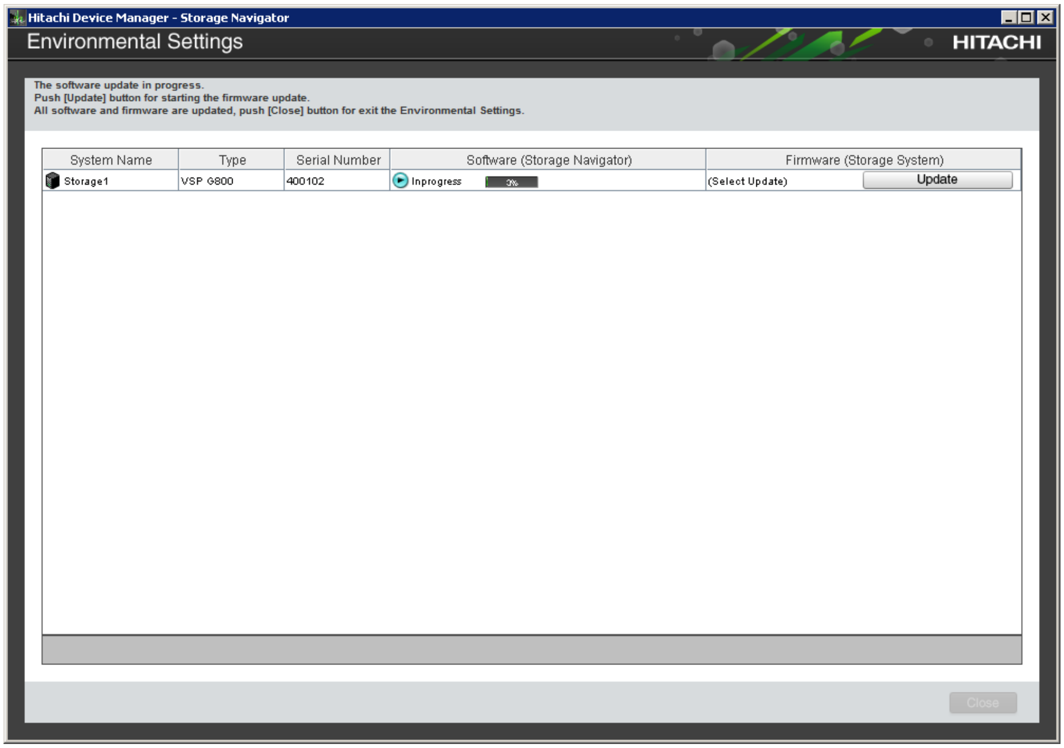
System Name	Type	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
unit0	VSP G800	300001	83-01-03-60/00 -> 83-01-20-60/02	83-01-20-60/00 -> 83-01-20-60/02

Selected: 1 of 1

14. To upgrade the firmware, click **Confirm** when the **Update software and firmware window** opens.

    The **Run Update Firmware** window opens and the upgrade starts automatically.

15. When the following screen opens, use the status bar under the **Software (Storage Navigator)** column to monitor the update status. The following table lists the status conditions.

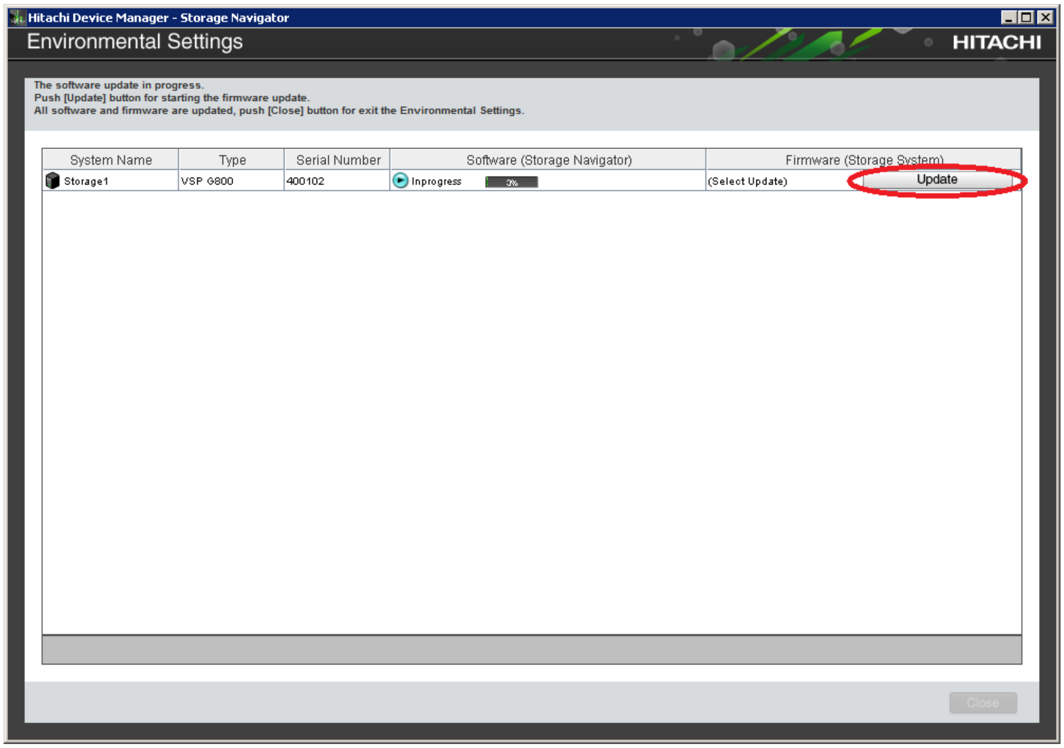


The software update in progress.
Push [Update] button for starting the firmware update.
All software and firmware are updated, push [Close] button for exit the Environmental Settings.

System Name	Type	Serial Number	Software (Storage Navigator)	Firmware (Storage System)
Storage1	VSP G800	400102	Inprogress 0%	(Select Update) Update

Status	Description
Waiting	One of the following: ▪ Software is not upgrading. ▪ Software components are being upgraded individually. If the software is already upgraded, this status refers to another storage system.
In progress	Software upgrade is running.
Completed	Software upgrade has completed.
Failed	One of the following: ▪ Software update failed. ▪ If storage systems were added, the addition might not be complete. Follow the on-screen instructions.
(Not Update)	This is not selected as a software update target. If storage systems were added, this status does not appear.

16. If you did not check **Firmware (Storage System)** in step 10, skip steps 15 through 18. Otherwise, update the firmware by clicking **Update** below the **Firmware (Storage System)** column.

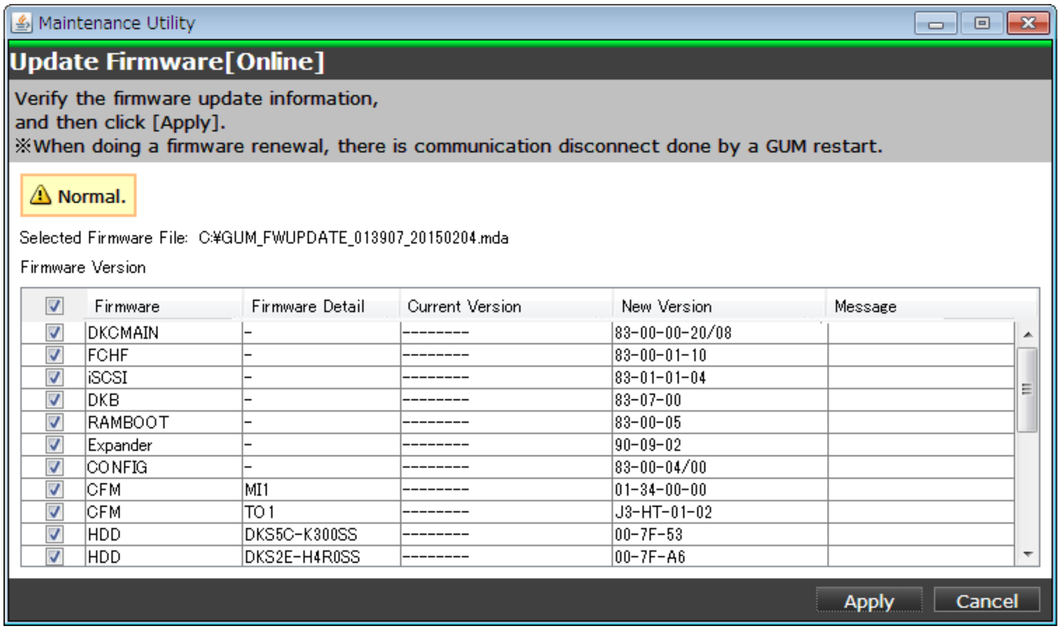


The software update in progress.
Push [Update] button for starting the firmware update.
All software and firmware are updated, push [Close] button for exit the Environmental Settings.

System Name	Type	Serial Number	Software (Storage Navigator)	Firmware (Storage System)
Storage1	VSP G800	400102	Inprogress 0%	(Select Update) Update

> **Note:** If a window reports a problem with this website's security certificate, click **Continue to this website**, and then close the browser. If a **Java Update Needed** window opens, click **Later**. If a JRE **Security Warning** window opens, select the check boxes in each window and click **Continue**, **Run**, or **Yes**.

17. When the **Update Firmware** window opens, click **Apply**.



Verify the firmware update information,
and then click [Apply].
※When doing a firmware renewal, there is communication disconnect done by a GUM restart.

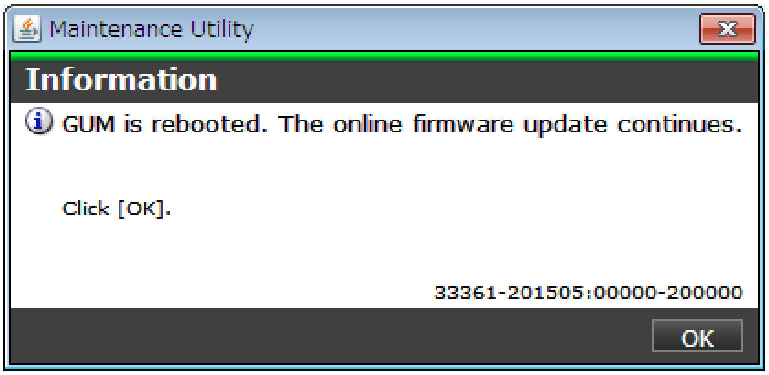
⚠ Normal.

Selected Firmware File: C:¥GUM_FWUPDATE_013907_20150204.mda

Firmware Version

☑	Firmware	Firmware Detail	Current Version	New Version	Message
☑	DKCMAIN	-	--------	83-00-00-20/08	
☑	FCHF	-	--------	83-00-01-10	
☑	iSCSI	-	--------	83-01-01-04	
☑	DKB	-	--------	83-07-00	
☑	RAMBOOT	-	--------	83-00-05	
☑	Expander	-	--------	90-09-02	
☑	CONFIG	-	--------	83-00-04/00	
☑	CFM	MI1	--------	01-34-00-00	
☑	CFM	TO1	--------	J3-HT-01-02	
☑	HDD	DKS5C-K300SS	--------	00-7F-53	
☑	HDD	DKS2E-H4R0SS	--------	00-7F-A6	

The **Update Firmware[Online]** window shows the status of the firmware upgrade. When the upgrade completes, the following window opens.



GUM is rebooted. The online firmware update continues.

Click [OK].

33361-201505:00000-200000

18. Click **OK**.

19. Wait for the firmware upgrade to complete, and then verify the firmware update status in the **Firmware (Storage System)** column of the **Environmental Settings** window. Wait for the firmware update to complete. The following table lists the status conditions.

Status	Description
(Select Update)	Click **Update** to display the **Update Firmware** window.
In progress	The **Update Firmware** window started and the firmware upgrade is not complete. This status appears even if the firmware upgrade is canceled.
Completed	Firmware upgrade is complete.
Failed	Firmware upgrade failed. Click **Update** to display the **Update Firmware** window, and review the error details.
Communication Timeout	The time[1] required to complete the firmware upgrade cannot be confirmed. Verify the state in the **Update Firmware** window.
(Not Update)	Not selected as a firmware upgrade target.
Note: 1. When NAS Modules are not installed, the installation time is approximately 3.5 hours. When NAS modules are installed, the installation time is approximately 9 hours.	

20. When the firmware upgrade completes, click **Close**.

Note: If the update firmware window is not displayed while registering the storage system on the SVP, terminate the procedure, and then register the storage system on the SVP again.

Chapter 17: Back up and restore the SVP

Best practices dictate that you back up the SVP configuration to a USB flash drive. That way, if the SVP fails, you can use the backup to restore the configuration.

Backing up the SVP configuration

Back up the SVP configuration to a USB flash drive using a Remote Desktop connection. After the configuration is backed up, you can use the back up to restore the configuration if necessary.

When you back up the SVP configuration, the following items are also backed up:

- Parameters set in the Device Manager - Storage Navigator Environment window
- Connection setting to the authentication server
- Connection setting to the key management server
- Password policy for backing up the encryption key on the client PC
- Window view setting (table width)
- Warning message in the logon window
- Task information
- SMI-S application settings
- HTTPS and SMI-S SSL certificates, and RMI

Procedure

1. From a management console PC, connect to the SVP using Windows Remote Desktop Connection.
2. Close all Device Manager - Storage Navigator sessions on the SVP.
3. On the SVP, exit to a Windows command prompt as Administrator.
4. Move to the directory where the tool exists, and then issue the following command:

```
C:\MAPP\wk\Supervisor\MappIniSet\MappBackup.bat [absolute path of the
backup (tgz zip) file]
```

> **Note:** In this command, `C:\MAPP` indicates the installation directory of the SVP. If the installation directory is different, replace `C:\MAPP` with the specified installation directory.

5. At the completion message, press any key to continue.

6. Exit the command prompt.
7. Move the configuration file from the SVP to a USB flash drive.

   Note: Do not edit the contents of the backup file.

Restoring the SVP configuration

If you backed up the SVP configuration, you can use the following procedure to restore the configuration. This procedure is particularly useful when you receive a replacement SVP and want to install a configuration that was used on your previous SVP.

Before you begin

- Verify the client PC is connected to the SVP through a Remote Desktop Connection.
- Check the storage system you want to restore is registered on the SVP.
- Configure the service setting to not start automatically when the SVP restarts.

Procedure

1. Copy the backup file to a folder on the SVP.
2. On the SVP, exit to a Windows command prompt as Administrator.
3. Move to the directory where the backup file exists, and then issue the following command:

   ```
   C:\MAPP\wk\Supervisor\MappIniSet\MappRestore.bat[absolute path of the
   backup (tgz zip) file]
   ```

   Note: In this command, `C:\MAPP` indicates the installation directory of the SVP. If the installation directory is different, replace `C:\MAPP` with the specified installation directory.
4. At the restoration message, press any key to continue.
5. Configure the service setting that you want to start automatically the next time the SVP restarts (see Changing storage system information in the Storage Device List).
6. Restart the SVP. Wait approximately 10 minutes for the restart to complete.

Chapter 18: Rebooting the SVP

There might be times when you need to shut down and restart the SVP.

Shutting down the SVP

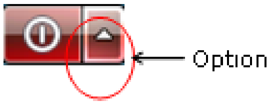
Procedure

1. On the SVP, click **Start** in the Windows desktop.
2. From the displayed menu, click **Windows Security**.
3. In the **Windows Security** window, click the up arrow option in the power menu.
4. From the displayed menu, click **Shut down**.
   If you have the physical SVP supplied by Hitachi Vantara, the `POWER` LED goes off.

Restarting the SVP

Procedure

1. On the SVP, click **Start** in Windows desktop.
2. From the displayed menu, click **Windows Security**.
3. In the **Windows Security** window, click the up arrow option in the power menu:

4. From the displayed menu, click **Reboot**.

Chapter 19: Replacing the Hitachi Vantara-supplied SVP

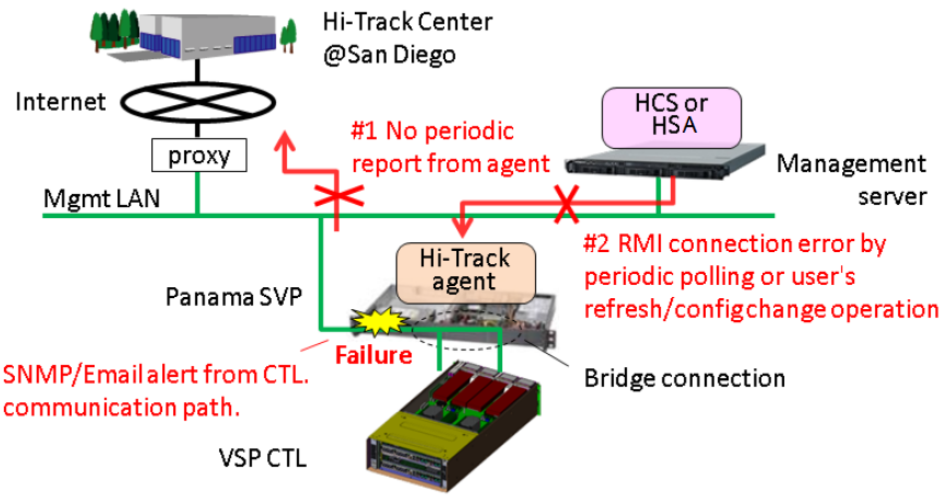
Use the following information to detect SVP failures and replace the physical SVP if necessary.

> **Important:** The Hitachi Vantara-supplied SVP can only be installed, upgraded, or replaced by a Hitachi Vantara representative or an authorized service provider. Contact a Hitachi Vantara representative for more information about installing, upgrading, or replacing a Hitachi Vantara-supplied SVP.

Detecting SVP failures

SVP failures are detected and resolved using the following methods.

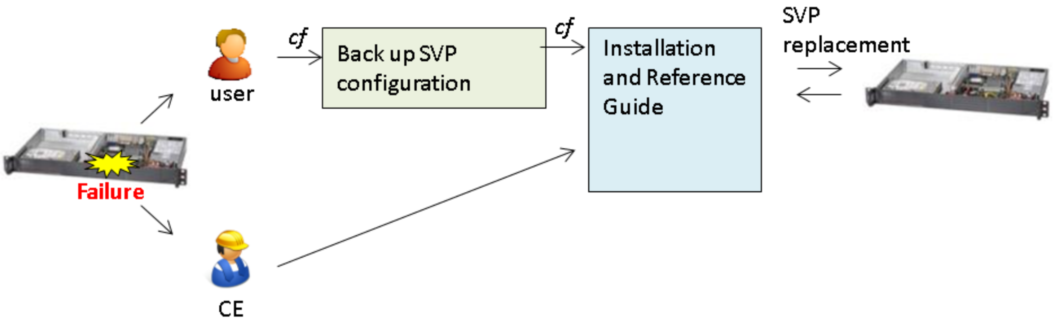
Failure detection method	How a failure is detected	Action to be taken
Hi-Track Remote Monitoring System	No report from the agent during a 24-hour health check	Hi-Track detects SVP failure -> SVP replacement. For information about Hi-Track, go to the Hi-Track website: http://hitrack.hds.com/.
Hitachi Command Suite (HCS)	RMI connection error (not alert)	See the *Hitachi Command Suite Administrator Guide* (MK-90HC175).
Hitachi Storage Advisor (HSA)	Hardware alerts appear in Alert tiles, along with drill-down views for detailed information.	See *Hitachi Storage Advisor User Guide* (MK-94HSA004).



Replacing the physical SVP

If the physical SVP supplied by Hitachi Vantara must be replaced, users back up the configuration and then return the failed SVP to Hitachi Vantara. When users receive the new SVP, they restore the configuration using the backup from the failed SVP.

The procedures for backing up and restoring the SVP configuration are in the Hardware Guide for your system.



Recovering the operating system

Recovery of the SVP operating system is achieved using Operating System Recovery Tool (OSRT).

The SVP supports OSRT as a backup solution for the C: partition. With this tool, users or CEs can back up the C: partition and restore it at any time, without requiring a USB. This tool can recover the SVP from OS or data corruption on the C:\ partition.

Backing up the OS

Procedure

1. Start the SVP.
2. At the Basic Input/Output System (BIOS) screen, press F8.
3. Select a partition for the backup.
4. Exit the BIOS and restart the SVP.

Restoring the OS

Procedure

1. Start the SVP.
2. At the BIOS screen, press F8.
3. Select an image to restore.
4. Exit the BIOS and restart the SVP.

Configuring the replacement physical SVP

If you receive a replacement physical SVP, prepare the SVP for use.

Procedure

1. Identify the local-area connection assignments for the SVP ports.
2. Rename the four internal SVP network adapters.
3. Configure the SVP for bridge mode or change the default TCP/IP settings of the SVP network ports for your subnet.
4. Install the Hitachi Device Manager - Storage Navigator software.
5. Install the Hi-Track Remote Monitoring system.

   Steps 1 through 4 are described in the procedures that follow. For information about installing Hi-Track, go to http://hitrack.hds.com/.

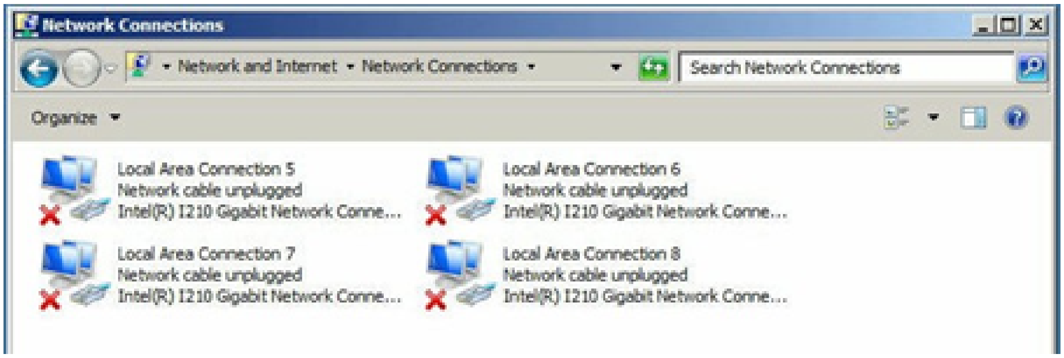
Mapping the internal SVP network adapters

The SVP has four internal network adapters that correspond to four external RJ-45 jacks. When you receive a new SVP, use the following procedure to assigning the adapters to Local Area Connection numbers.

Procedure

1. If any LAN cables are connected to the SVP ports, disconnect them.
2. Click **Control Panel** > **Network and Sharing Center**.
3. Click **Change adapter settings**.

4. Verify that all four SVP LAN adapters are recognized, but disconnected, and that the local-area connection numbers are assigned as 5, 6, 7, and 8.


Network Connections
Network and Internet ▸ Network Connections
Search Network Connections
Organize

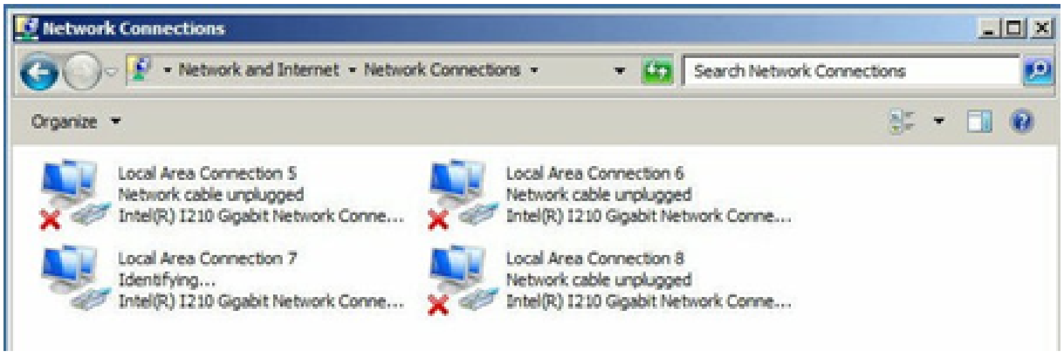
Local Area Connection 5
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 6
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 7
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 8
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

5. Connect an Ethernet cable to the LAN1 port on the SVP.
Local Area Connection 7 is assigned to the LAN1 port.


Network Connections
Network and Internet ▸ Network Connections
Search Network Connections
Organize

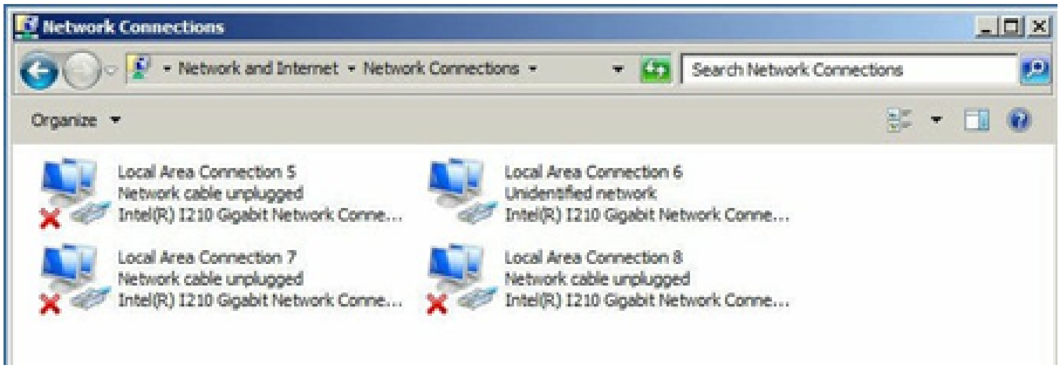
Local Area Connection 5
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 6
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 7
Identifying...
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 8
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

6. Remove the Ethernet cable from the LAN1 port and connect it to the LAN2 port on the SVP.
Local Area Connection 6 is assigned to the LAN2 port.


Network Connections
Network and Internet ▸ Network Connections
Search Network Connections
Organize

Local Area Connection 5
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 6
Unidentified network
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 7
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

Local Area Connection 8
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

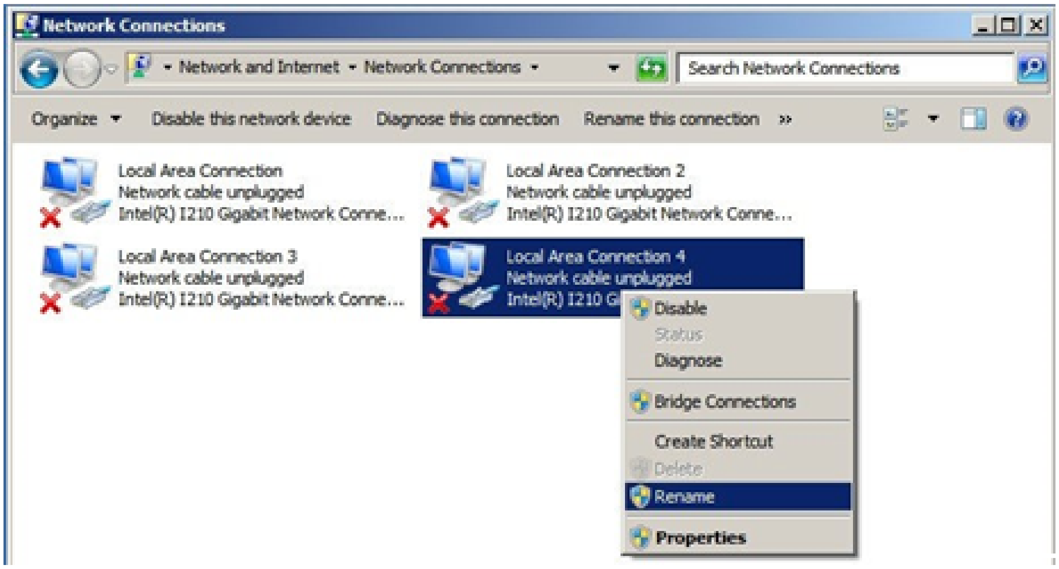
7. Repeat step 6 with the LAN3 and LAN4 ports on the SVP.
When you connect the Ethernet cable to these ports, Local Area Connection 8 will be assigned to the LAN3 port and Local Area Connection 5 will be assigned to the LAN4 port.

> **Note:** Verify that no IP address is configured for the SVP LAN ports. Otherwise, the storage system could become blocked.

Renaming the internal SVP network adapters

Procedure

1. Right-click LAN1 (Local Area Connection 4), and then click **Rename**.



2. Change the name to `Management(User)`.
3. Repeat step 1 and step 2 to rename the other three SVP network adapters as follows.

Change the name of this SVP adapter...	...to this name	Adapter configuration
LAN1	Management(User)	Bridge for the management LAN
LAN2	Maintenance	Maintenance LAN
LAN3	Management(CTL1)	Management LAN
LAN4	Management(CTL2)	Bridge for the management LAN

4. Leave the **Network Connections** window open. Then either configure the SVP for bridge mode or configure the IP addresses for the SVP LAN ports to match the IP addressing scheme of your subnet.

Setting the IP address

After renaming the internal SVP network adapters, perform the initial startup procedures to specify the IP addresses for the SVP and storage system.

⚠ **Caution:** Do not connect network servers such as the proxy between the client PC, SVP, and the storage system.

Procedure

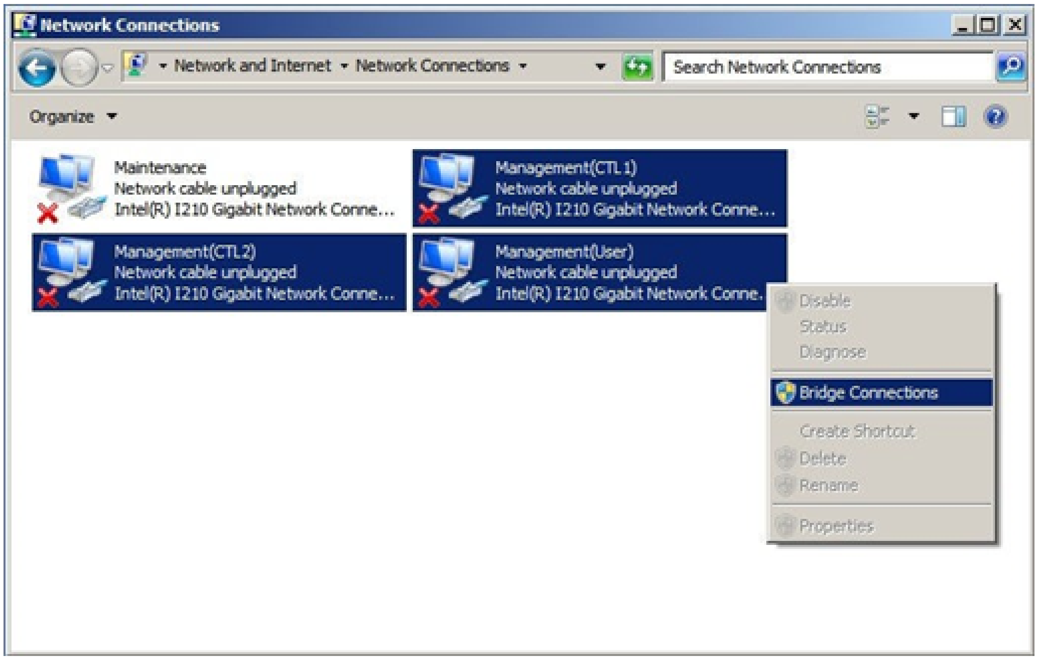
1. Connect a PC to the LAN2 port on the SVP.
2. Log on to the SVP using the Remote Desktop Connection:
   a. Configure the PC to use an IP address of 10.0.0.xxx, where xxx = 1-99 or 101-254, and a subnet mask of 255.255.255.0.
   b. Click **Start** > **All Programs**, and then click **Accessories** > **Remote Desktop Connection**.
   c. In the **Computer** field, type `10.0.0.100` and click **Connect**.
   d. In the **Windows Security** screen, type `SVP-PC\SVP` in the top field and `raid-login` in the bottom field.
   e. Click **OK**.
   f. If prompted that the identity of the remote computer cannot be verified, click **Yes** to continue.
3. In the Remote Desktop Connection window, click **Control Panel** > **Network and Sharing Center**.
4. Click **Change adapter settings**.
5. In the **Network Connections** window, right-click the **Management(CTL1)** network adapter, which corresponds to SVP physical port LAN3, and click **Properties**.
6. In the **Local Area Connection Properties** window, double-click **Internet Protocol version 4 (TCP/IPv4)** or **Internet Protocol version 6 (TCP/IPv6)**, depending on the IP addressing schemes used on your subnet.
7. In the dialog box, click **Use the following IP address**.
8. Enter the IP address, subnet mask, and gateway settings in the appropriate fields, and then click **OK**.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. In the **Network Connections** window, right-click the **Management(CTL2)** network adapter, which corresponds to the LAN4 port on the physical SVP, and click **Properties**. Then repeat steps 3 through 7 to assign the TCP/IP settings for this network adapter.
11. Close the **Network connections** window.

Configuring bridge settings

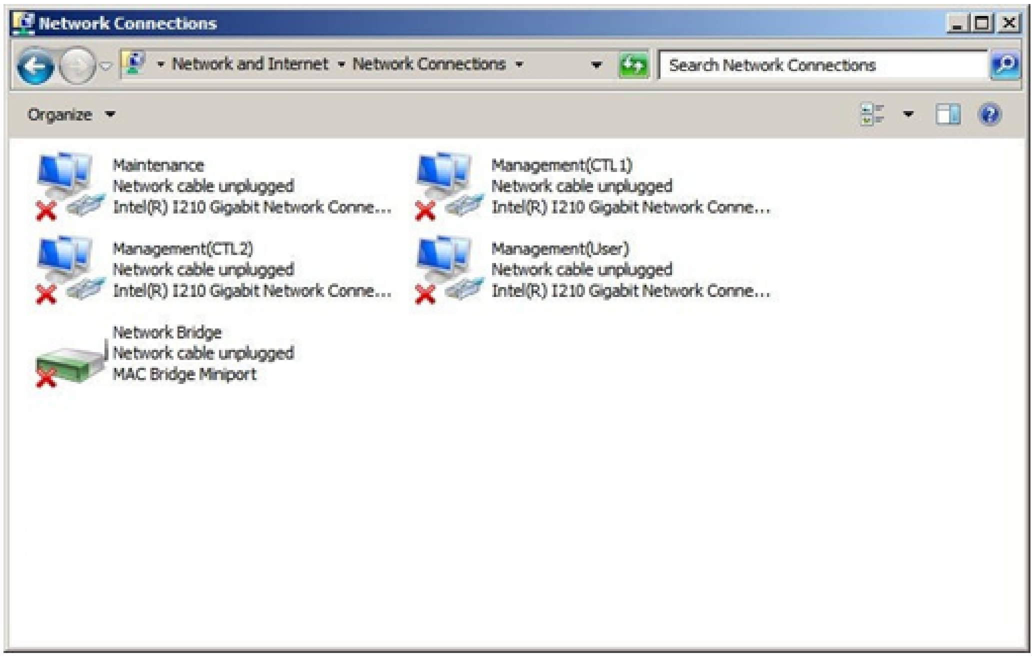
If your environment requires the SVP to operate in bridge mode, you can configure the SVP to operate in bridge mode after you rename the four internal SVP network adapters. In this mode, SVP ports LAN3 and LAN4 connect to the LAN management port on each controller.

Procedure

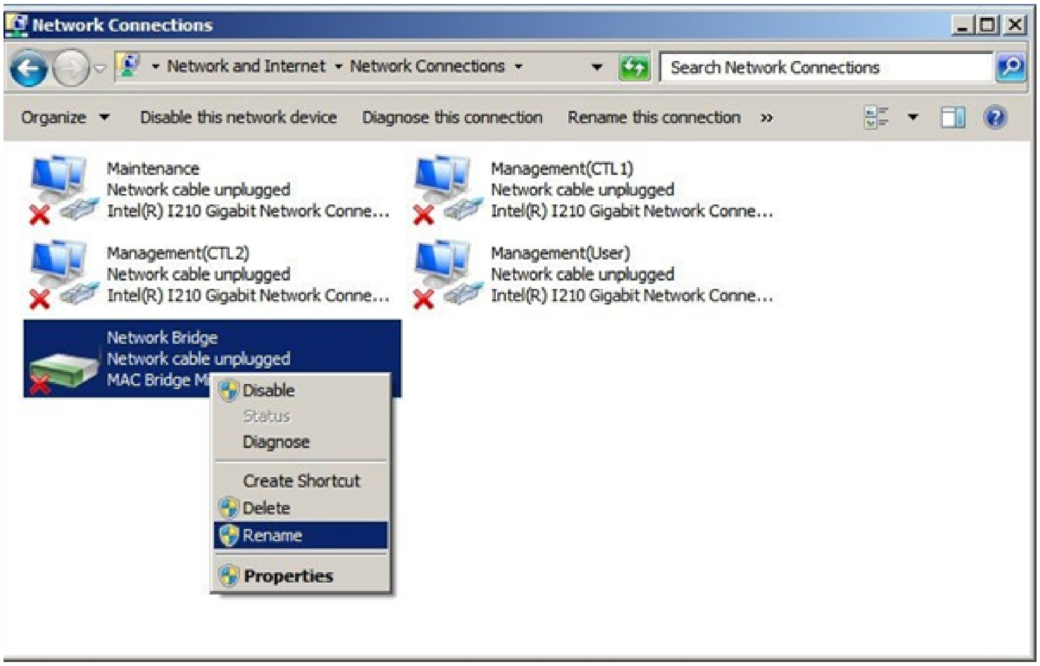
1. In the **Network Connections** window, click the LAN1 adapter, and then hold down the Ctrl key and click the LAN3 and LAN4 network adapters.
2. Right-click the mouse and click **Bridge Connections**.



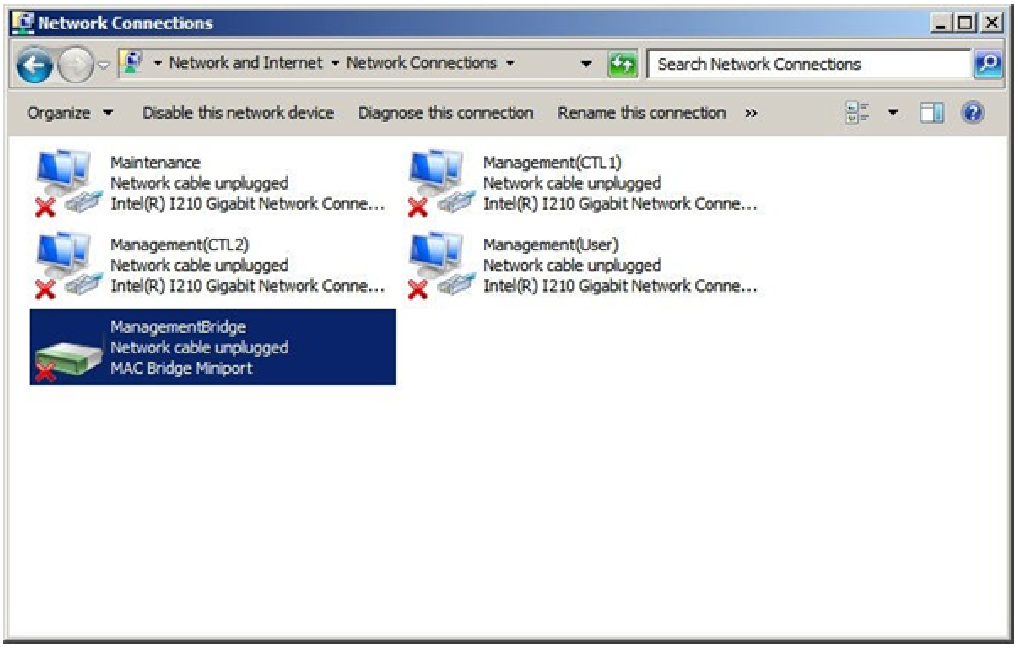
A new instance of Network Bridge appears.



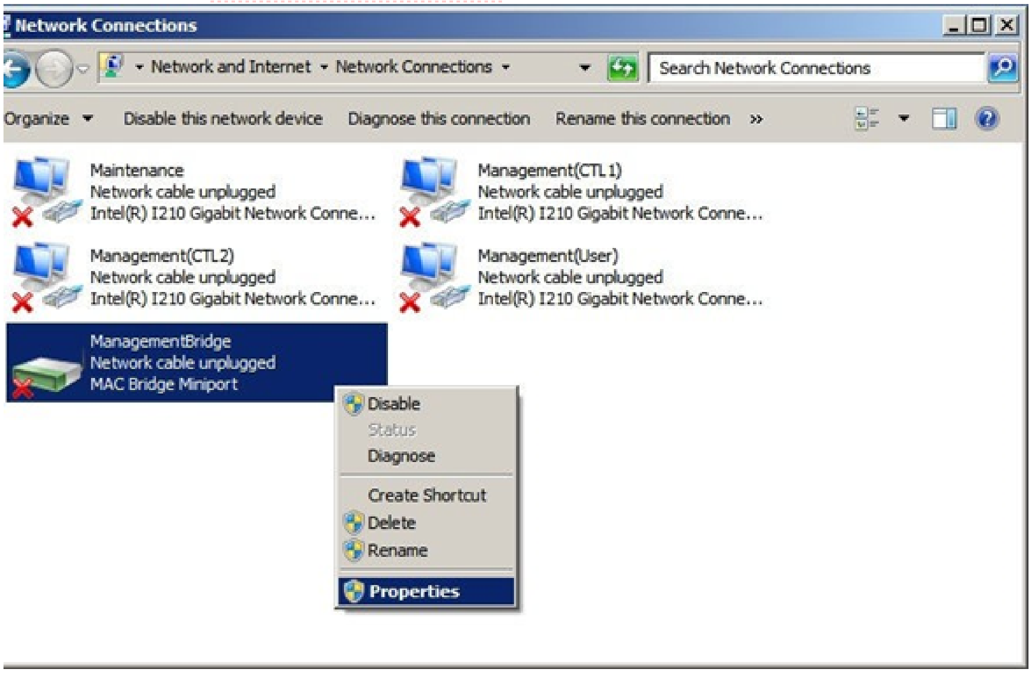
3. Right-click the **Network Bridge** icon, and then click **Rename**.



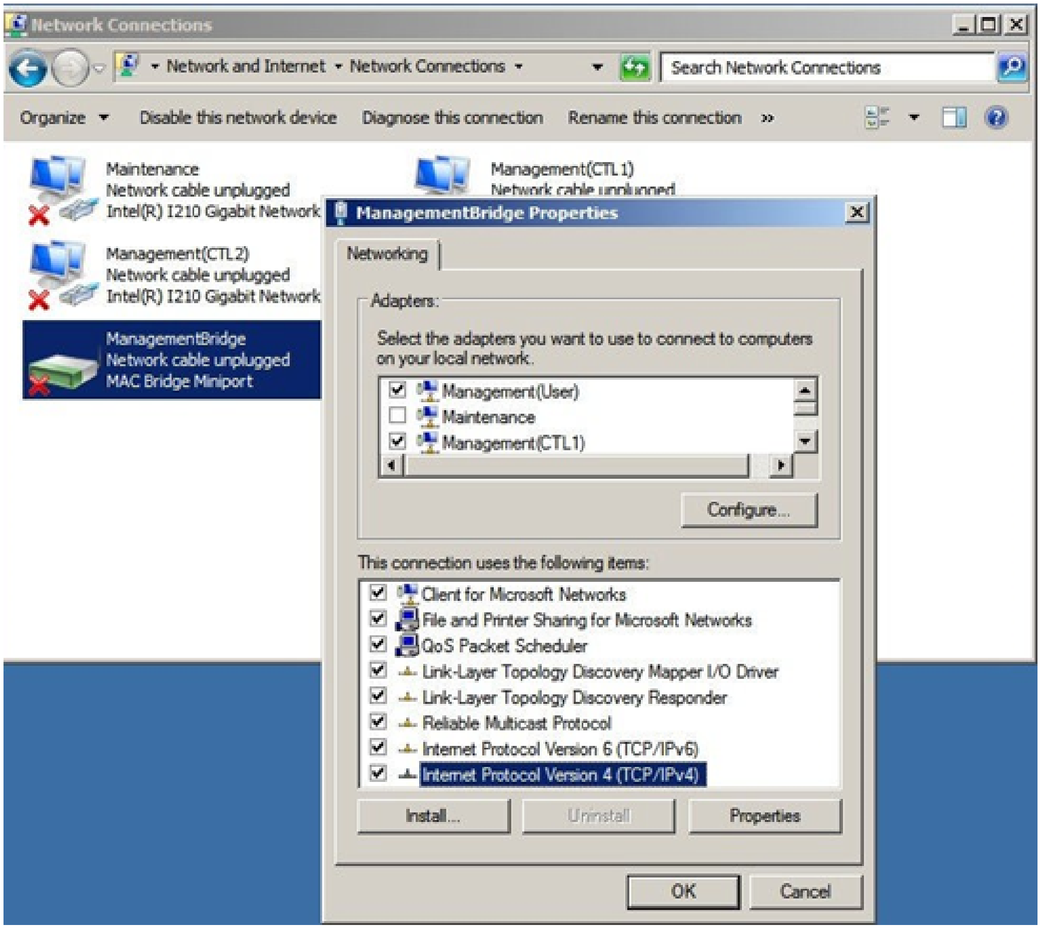
4. Change the name to `ManagementBridge`. Type this name as one word, with no spaces.



5. Right-click the **ManagementBridge** icon, and then click **Properties**.



6. Click **Internet ProtocolVersion 4 (TCP/IPv4)**.



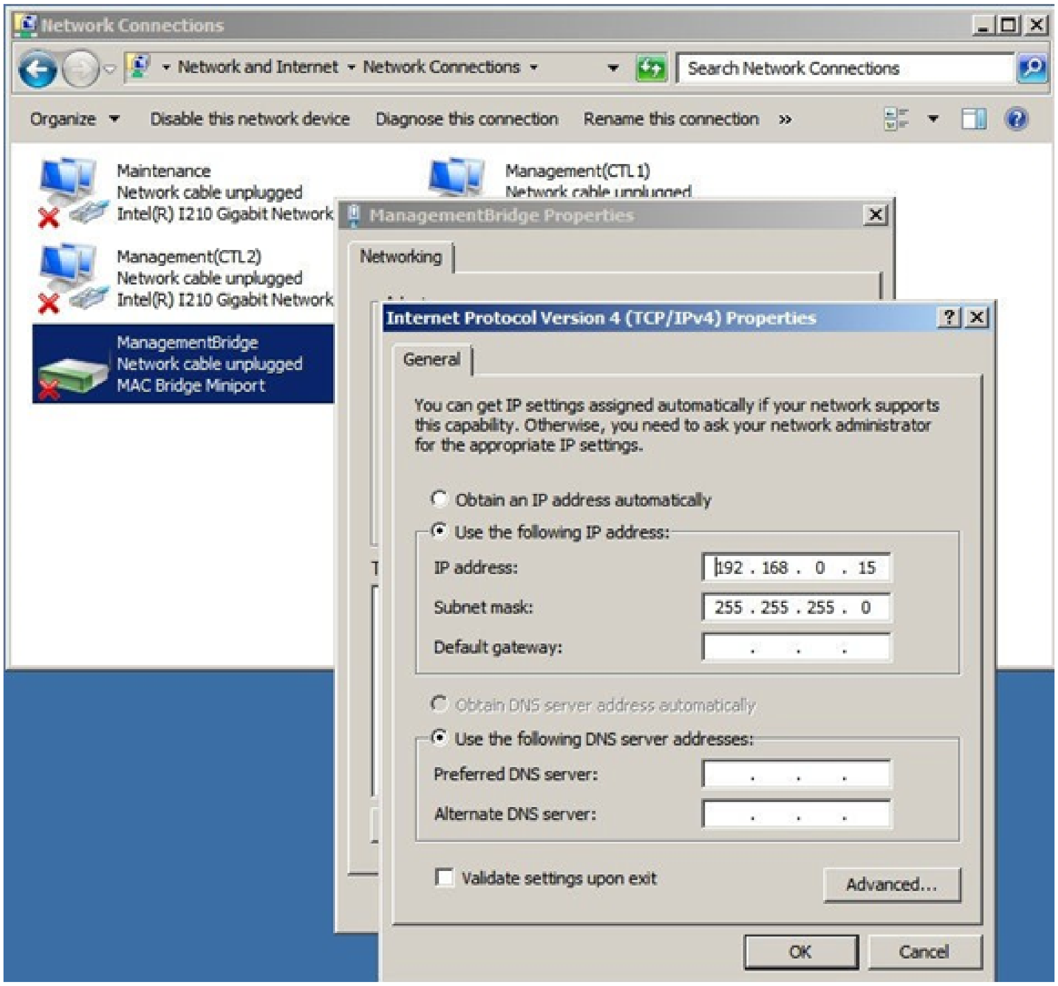
Select the adapters you want to use to connect to computers on your local network.

- ☑ Management(User)
- ☐ Maintenance
- ☑ Management(CTL1)

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Reliable Multicast Protocol
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

7. Configure the following IP settings for **ManagementBridge**:
   - IP address : 192.168.0.15 (default)
   - Subnet mask: 255.255.255.0



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 15

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

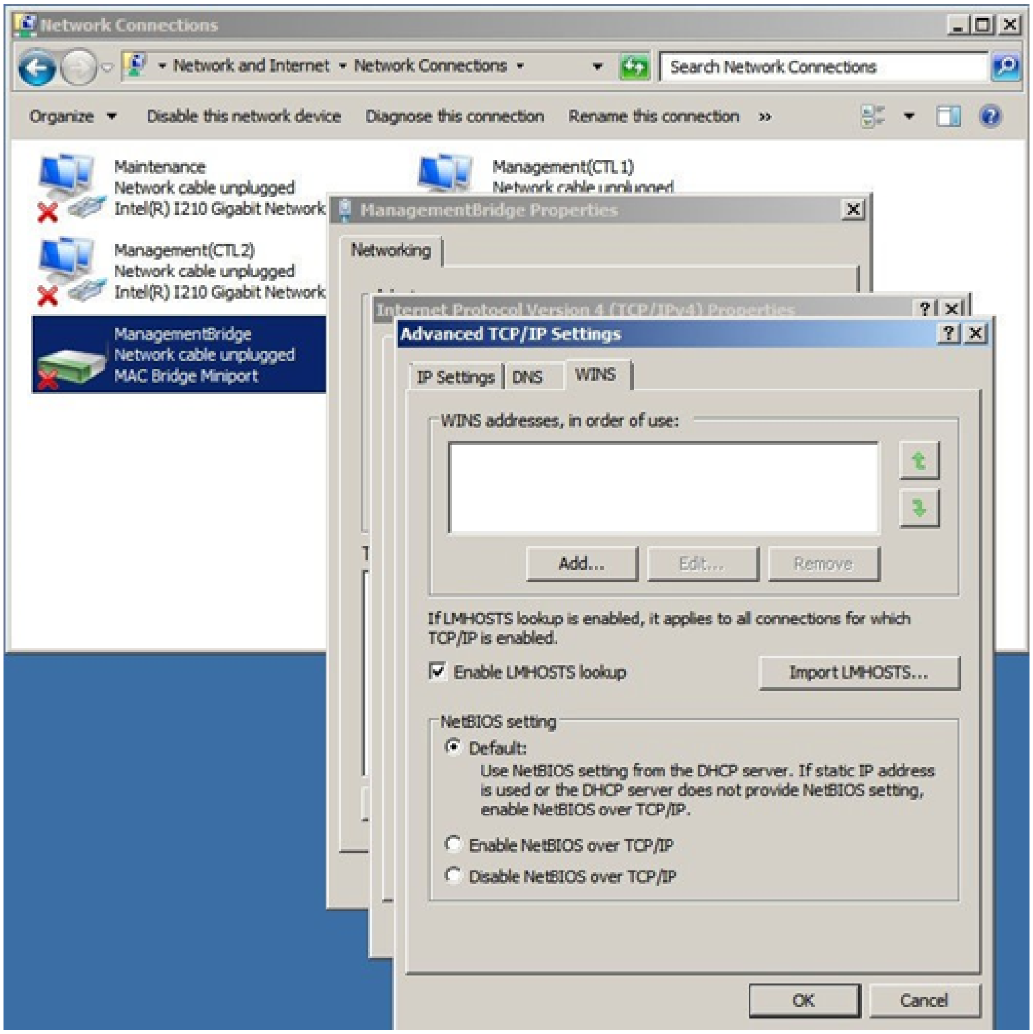
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

8. Click **Advanced**, and then click the **WINS** tab.



WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

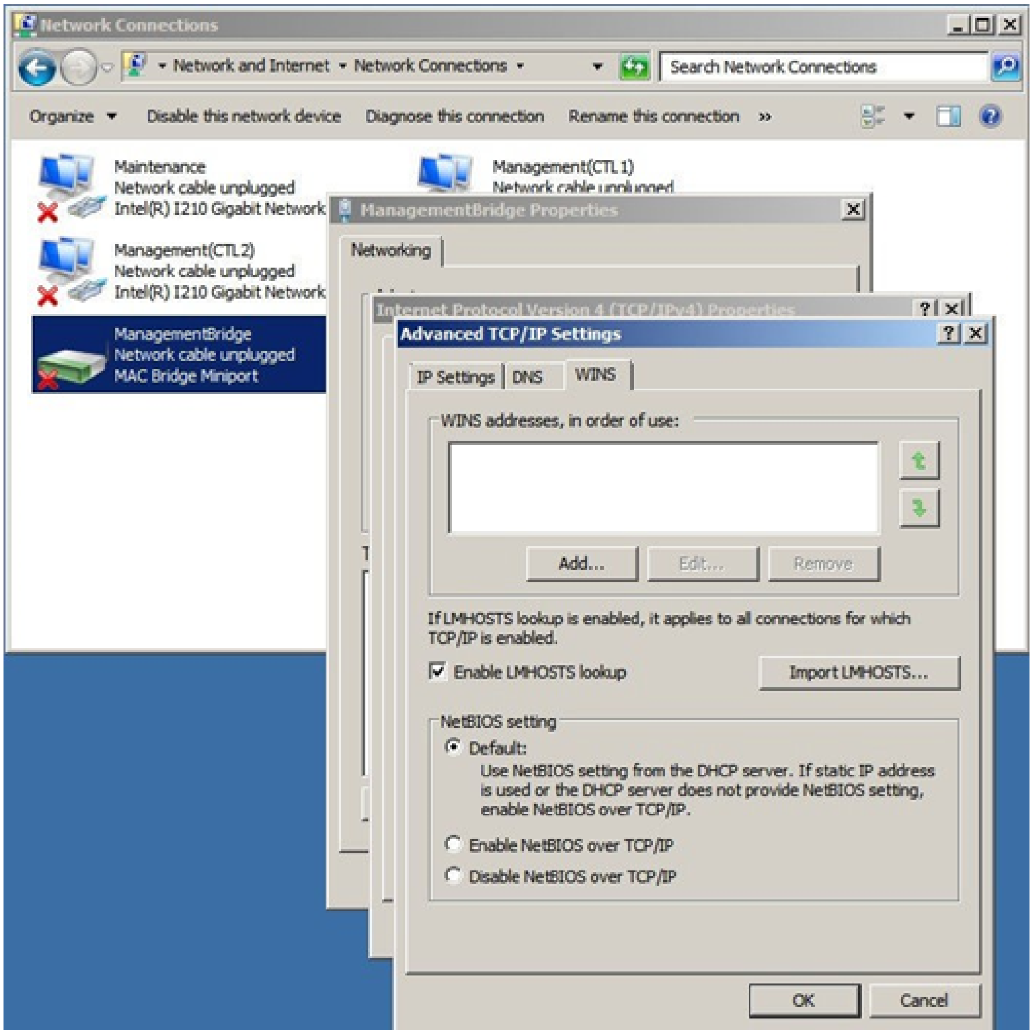
● Default:

Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

9. Under **NetBIOS setting**, click **Disable NetBIOS over TCP/IP**, and then click **OK**.



WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

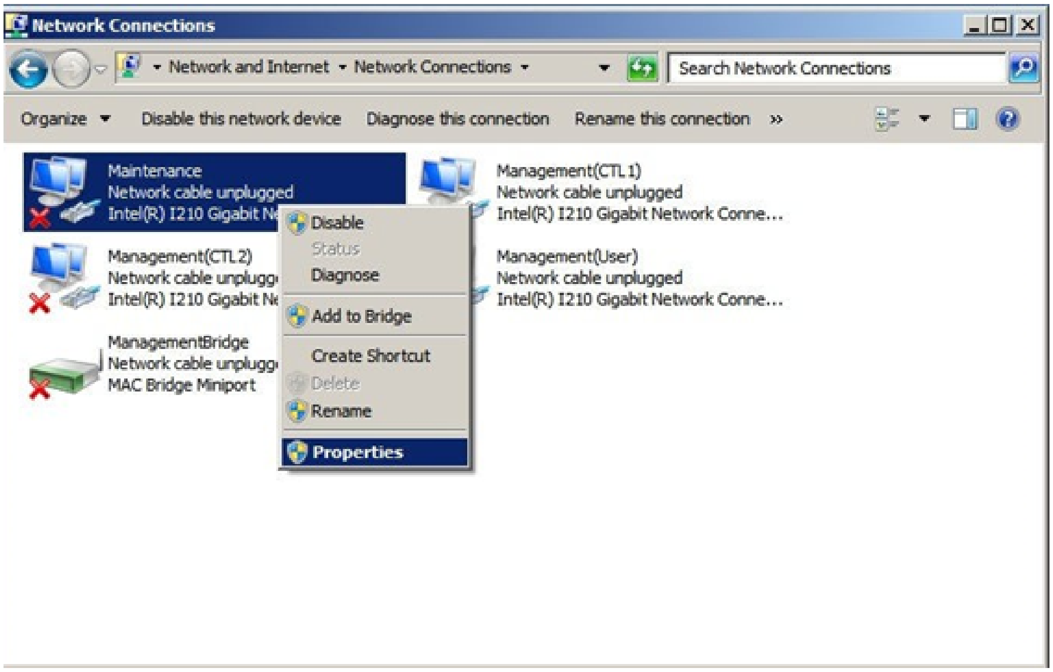
● Default:

Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

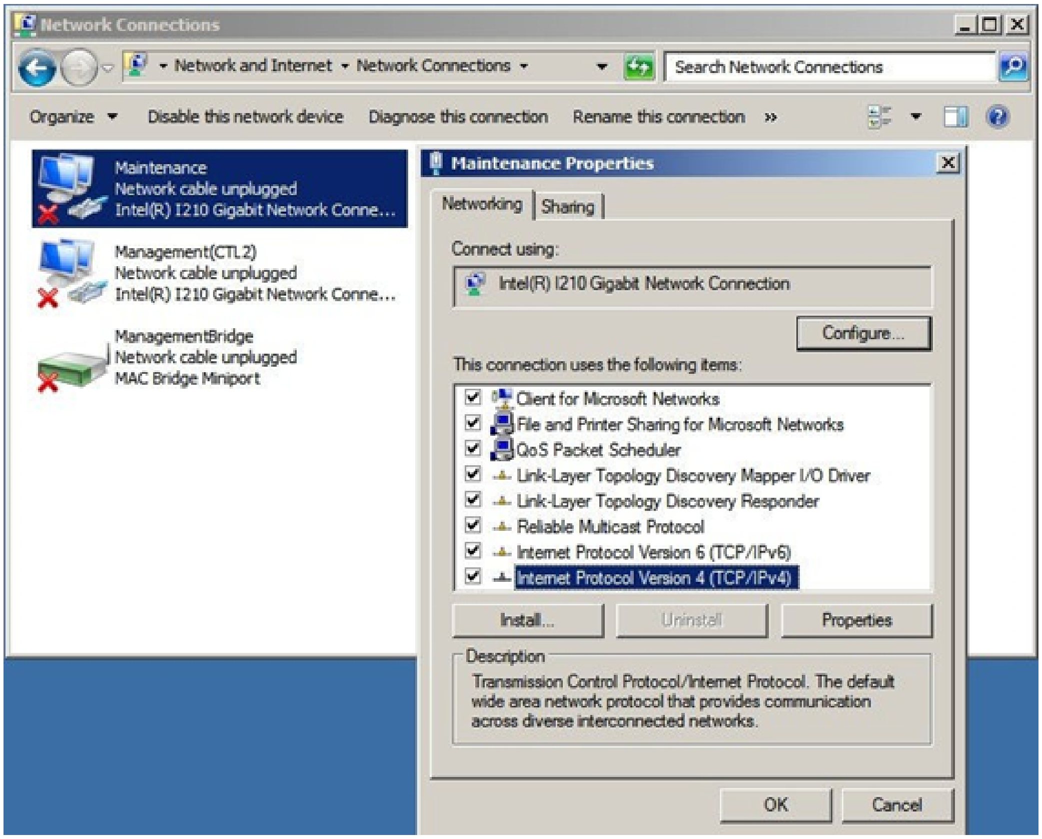
○ Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

10. Right-click the **Maintenance** icon (LAN2), and then click **Properties**.



11. Click **Internet ProtocolVersion 4 (TCP/IPv4)**.



Connect using:

Intel(R) I210 Gigabit Network Connection

This connection uses the following items:

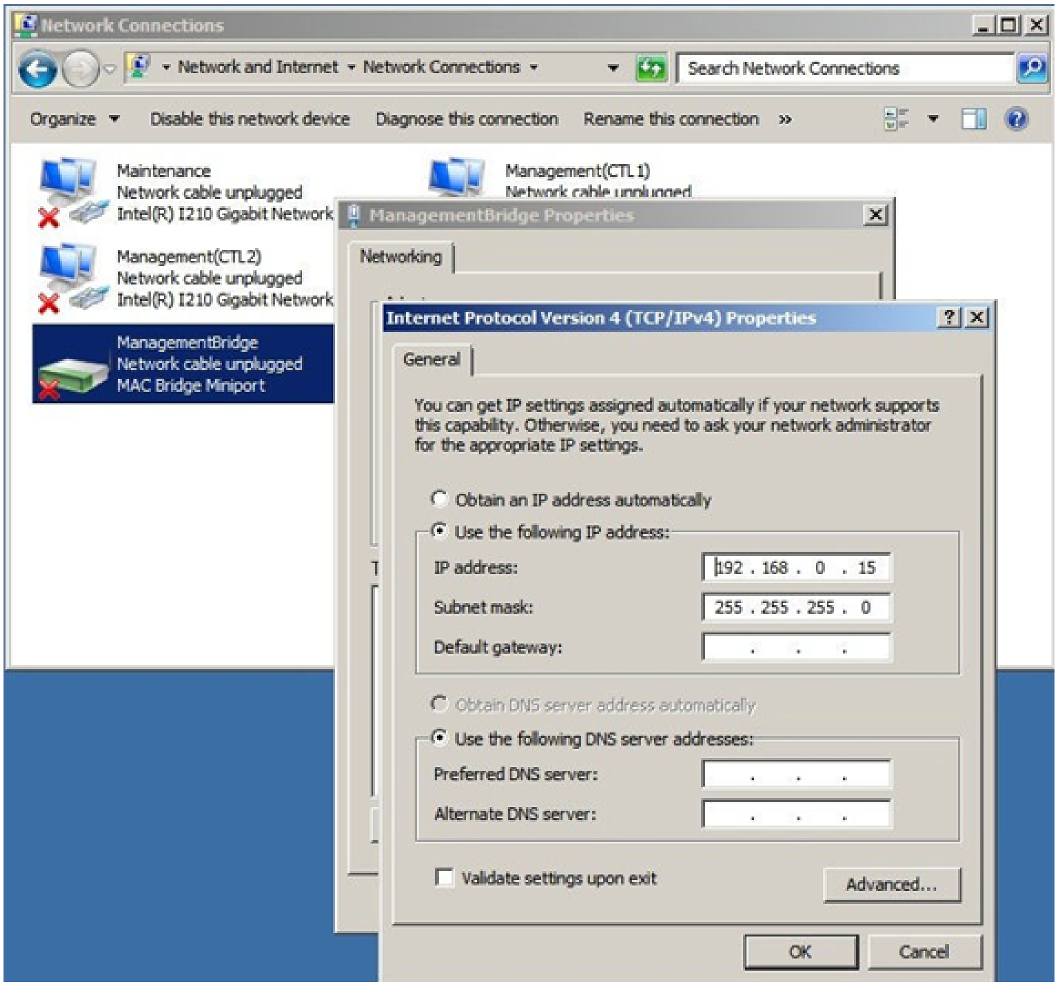
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Reliable Multicast Protocol
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

12. Configure the following IP settings for **Maintenance** (LAN2):

- IP address : 10.0.0.100 (default)
- Subnet mask: 255.255.255.0



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 0 . 15
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

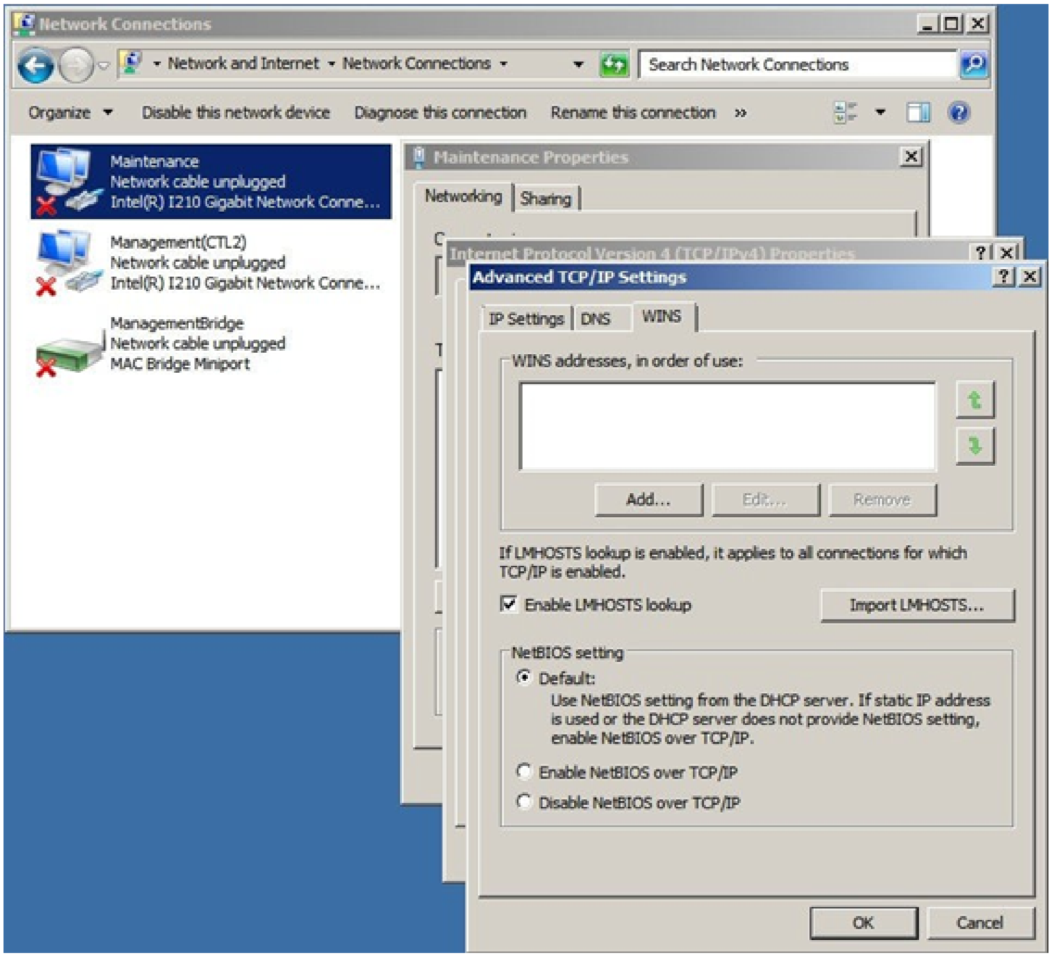
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

13. Click **Advanced**, and then click the **WINS** tab.



Maintenance
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

Management(CTL2)
Network cable unplugged
Intel(R) I210 Gigabit Network Conne...

ManagementBridge
Network cable unplugged
MAC Bridge Miniport

WINS addresses, in order of use:

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

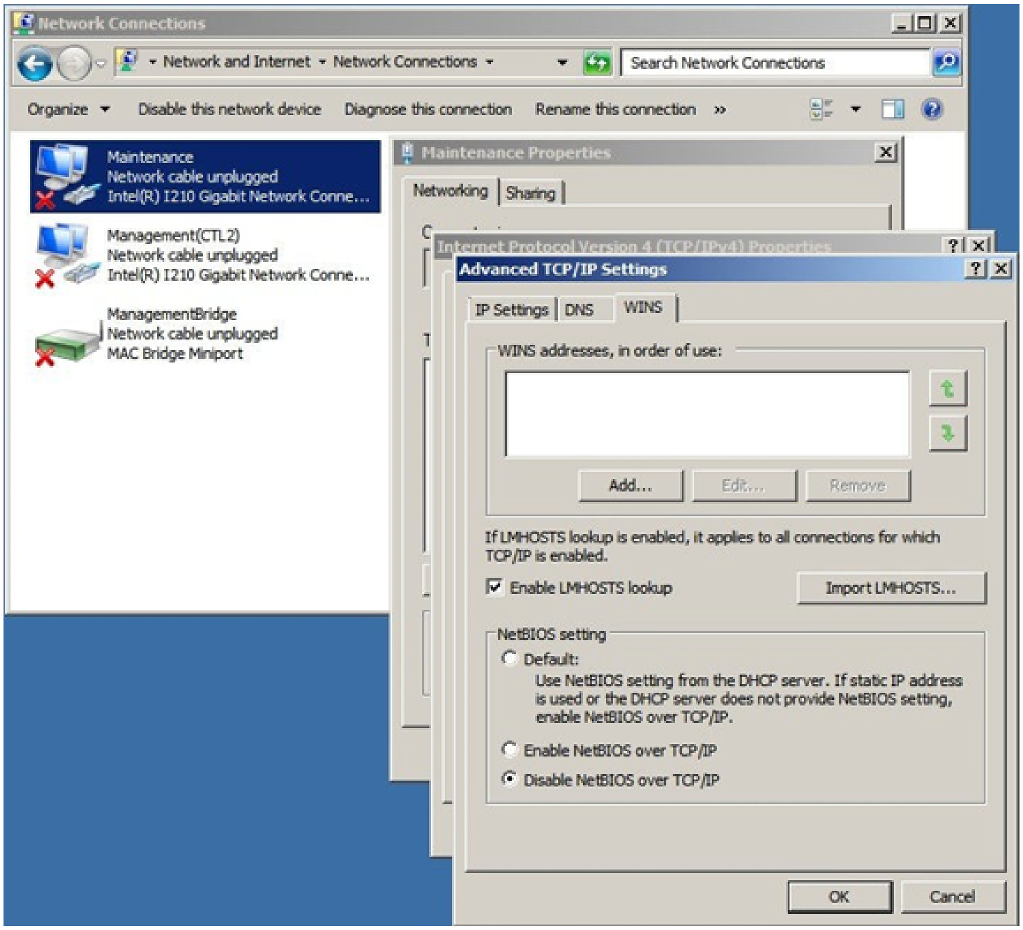
● Default:

Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

14. Under **NetBIOS setting**, click **Disable NetBIOS over TCP/IP**, and then click **OK**.



If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

NetBIOS setting

○ Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

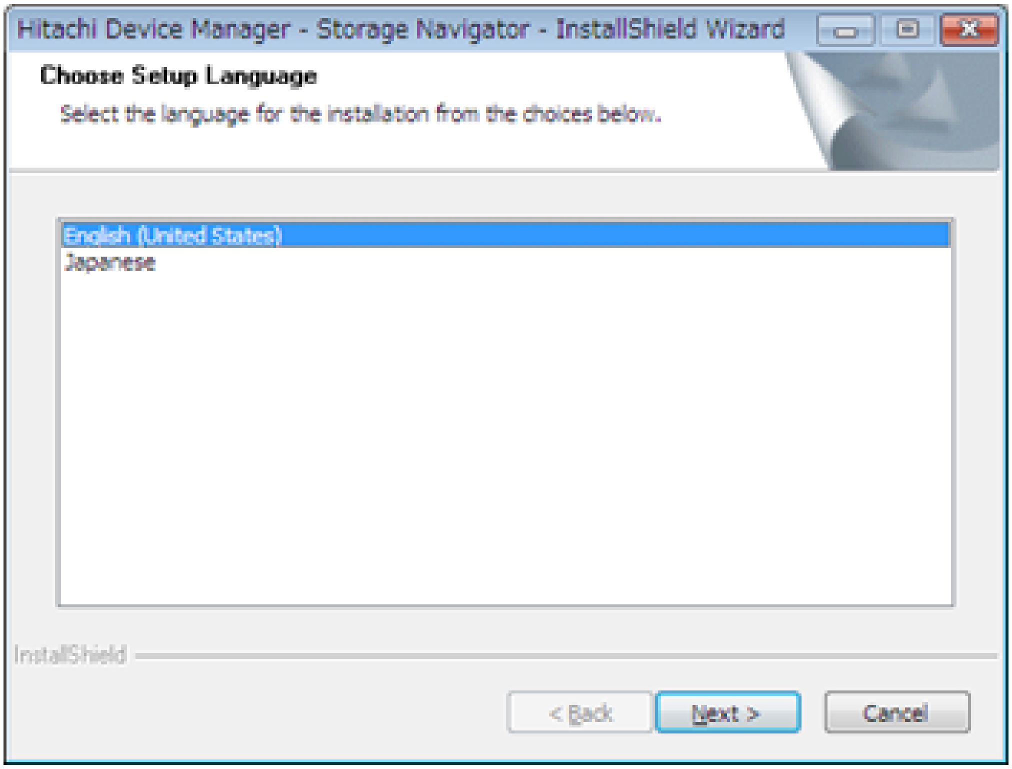
15. Click **OK** to apply the settings and close the **Local Area Connection Properties** window.
16. Close the **Network Connections** window.

Installing Hitachi Device Manager - Storage Navigator

The procedure for installing the Device Manager - Storage Navigator software takes approximately 10 minutes.

Procedure

1. Connect a PC to the LAN2 port on the SVP.
2. Insert the attached SVP firmware media into the PC's CD drive or DVD drive.
3. On the root folder of the SVP firmware media, right-click **Setup.exe**, and then click **Execute as Administrator**.
4. In the **Choose Setup Language** window, click a language, and then click **Next**.



Hitachi Device Manager - Storage Navigator - InstallShield Wizard

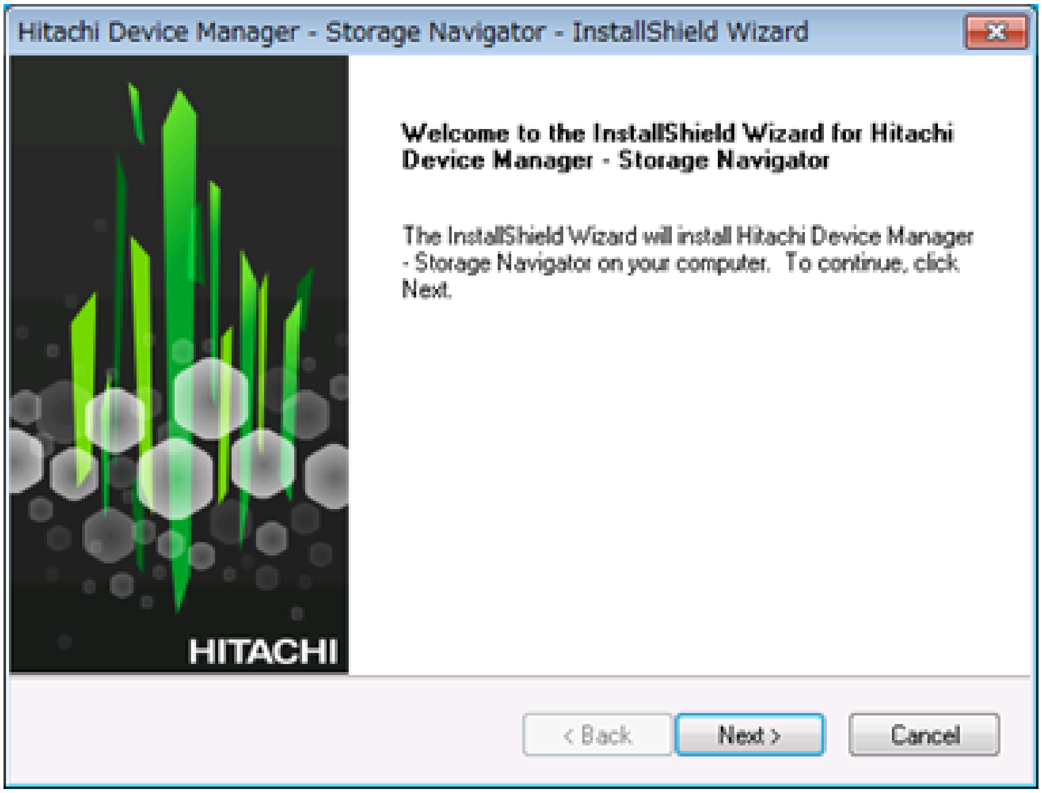
Choose Setup Language

Select the language for the installation from the choices below.

English (United States)
Japanese

The **Preparing Setup** window appears while the software is prepared for installation.

5. At the **Install Shield** window, click **Next**.

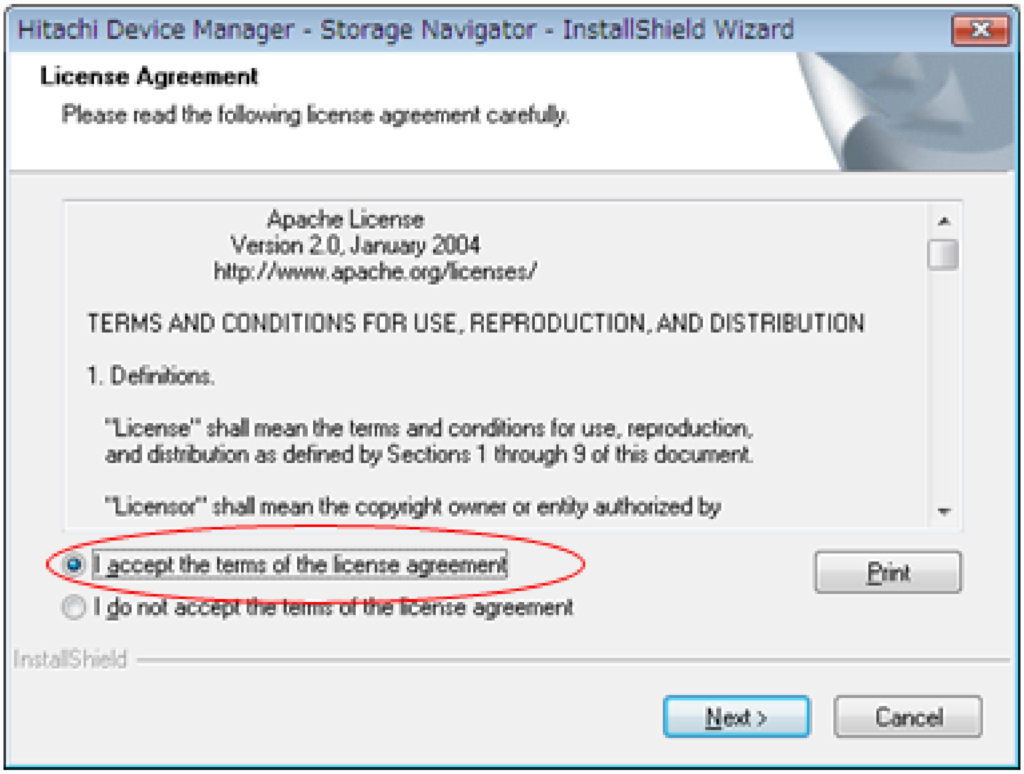


Hitachi Device Manager - Storage Navigator - InstallShield Wizard

Welcome to the InstallShield Wizard for Hitachi Device Manager - Storage Navigator

The InstallShield Wizard will install Hitachi Device Manager - Storage Navigator on your computer. To continue, click Next.

6. At the **License Agreement** window, accept the terms of the license agreement, and then click **Next**.



Hitachi Device Manager - Storage Navigator - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

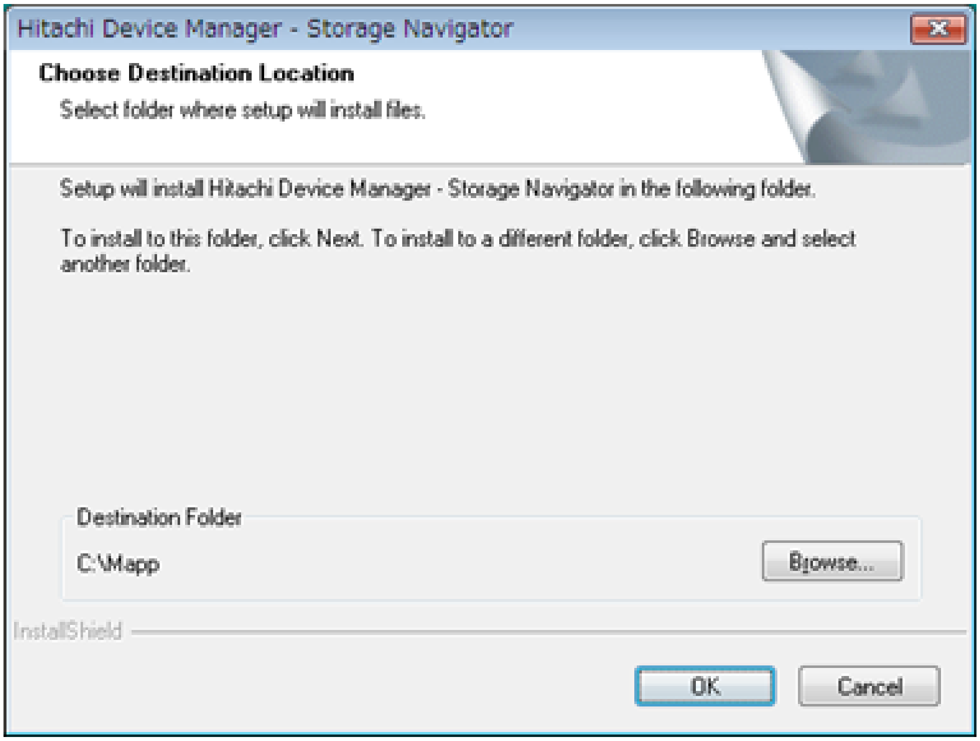
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

7. At the next window, specify the folder where Device Manager - Storage Navigator will be installed. Either accept the default folder shown in the window or click **Browse** to select a different folder.



Hitachi Device Manager - Storage Navigator

Choose Destination Location

Select folder where setup will install files.

Setup will install Hitachi Device Manager - Storage Navigator in the following folder.

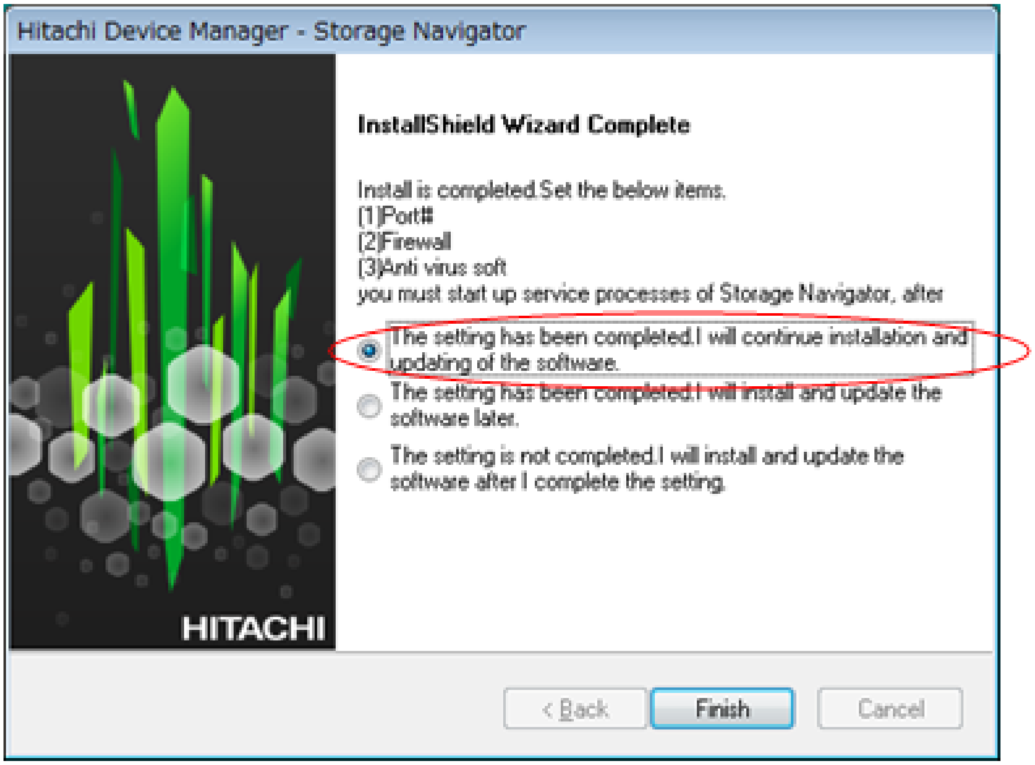
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Mapp

8. If a confirmation window appears, click **Yes**. If the Windows Security Alert window appears, click **Allow access**.
   A status bar shows the progress of the installation.

9. When the following completion message appears, perform one of the following steps:
   - To continue, click **The setting has been completed. I will continue installation and updating of the software.**
   - To set port numbers, firewall settings, and anti-virus software, click **The setting is not completed. I will install and update the software after I complete the setting.**



Hitachi Device Manager - Storage Navigator

InstallShield Wizard Complete

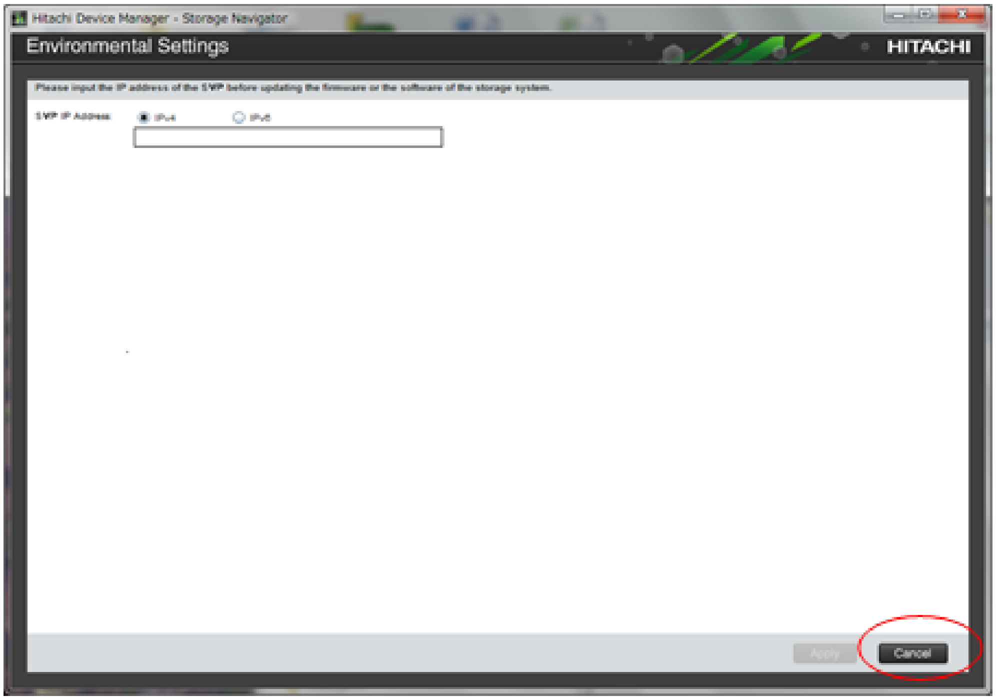
Install is completed.Set the below items.
(1)Port#
(2)Firewall
(3)Anti virus soft
you must start up service processes of Storage Navigator, after

● The setting has been completed.I will continue installation and updating of the software.

○ The setting has been completed.I will install and update the software later.

○ The setting is not completed.I will install and update the software after I complete the setting.

10. Click **Finish**.
11. At the **Environmental Settings** window, click **IPv4** or **IPv6**, and then enter the IP address of the SVP and click **Apply**.



Please input the IP address of the SVP before updating the firmware or the software of the storage system.

SVP IP Address: ● IPv4 ○ IPv6

Note: If you do not want to configure the SVP IP address at this time, click **Cancel**. When you are ready to specify the IP address, restart the SVP, and then set the SVP IP address using the procedure under Setting the IP address (on page 170) .

Chapter 20: Troubleshooting

In the unlikely event you encounter a problem with the SVP, use this information to identify and resolve the issue.

Troubleshooting the spanning tree protocol

To identify redundant paths, the SVP generates and processes Bridge Protocol Data Units (BPDUs) on ports 1, 3, and 4. If the SVP connects to a network switch that has its spanning tree feature enabled, the network switch can block communications between the SVP and the network. An example of a configuration is Cisco switches equipped with the PortFast BPDU guard feature is enabled.

If you connect the SVP to the port of a network switch that has BPDU guard enabled, connect the SVP to a different port on the switch that does not have the BPDU guard feature enabled. If this does not resolve the problem, perform the following procedure to stop the SVP port from issuing BPDU frames.

Note: If you perform this procedure while the cable connection between the SVP and network switch is looped, it creates a logical loop of the network connection and the entire network becomes inoperable. Verify the network connection is not looped before performing this procedure.

Procedure

1. From the PC connected to the SVP, click **Start** > **All Programs > Accessories > Remote Desktop Connection**.
2. Right-click the command prompt and click **Run as Administrator**.
3. At the command prompt, type `regedit`.
4. Edit the following registry settings:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BridgeMP`

   Name: `DisableSTA`

   Value: `DWORD(0x1)`
5. Restart the SVP operating system. The SVP port no longer transmits BPDU frames.

SVP emergency logon procedure

The SVP can be connected using the default IP address 192.168.0.15.

If you cannot connect to the SVP by using the default IP address, use the following emergency log on address: `http://<default SVP IP address>/dev/storage/<model number><system serial number>/emergency.do`. The following table lists the variables in the URL.

If your storage system model number is ...	... and the storage system serial number is ...	... type the following URL
8320004	456789	http://192.168.0.15/dev/storage/8320004456789/emergency.do
8340004	456789	http://192.168.0.15/dev/storage/8340004456789/emergency.do
8360004	456789	http://192.168.0.15/dev/storage/8360004456789/emergency.do

Appendix A: SVP replacement list

The following table lists the product codes for replacement SVPs.

Component	Available for VSP model	Product code
Service processor (Windows 10 Enterprise)	VSP G350 and VSP G370 VSP F350 and VSP F370	HDW2-F850-SVP.P
	VSP G700 VSP F700	
	VSP G900 VSP F900	HDW-F850-SVP.P
	VSP G200	HDW2-SVP2OS10.P
	VSP G400, G600, G800	HDW-SVP2OS10.P
	VSP F400, F600, F800	FHW-SVP2OS10.P
Service processor (Windows 7)	VSP G200	3919435-HDW2.P
	VSP G400, G600, G800	3919435.P
	VSP F400, F600, F800	H3919435.P

Hitachi Vantara

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-5474526
HitachiVantara.com/contact