HITACHI
Inspire the Next

Hitachi Virtual Storage Platform E990

Hitachi Virtual Storage Platform Gx00 and Fx00

Hitachi Virtual Storage Platform Nx00

Service Processor Technical Reference

This guide is intended for system administrators, Hitachi Vantara representatives, and authorized service providers and provides information about setting up, configuring, and maintaining both physical and virtual service processors.

MK-97HM85045-05
April 2020

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 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 URL for the Hitachi Interoperability Reports website.

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 LLC.

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 the latest SVP versions and platforms supported, see https://support.hitachivantara.com/en/user/answers/interoperability.html.

Chapter 2: 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 (Windows 10 Enterprise) 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 1 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 (Windows 10 Enterprise) 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.

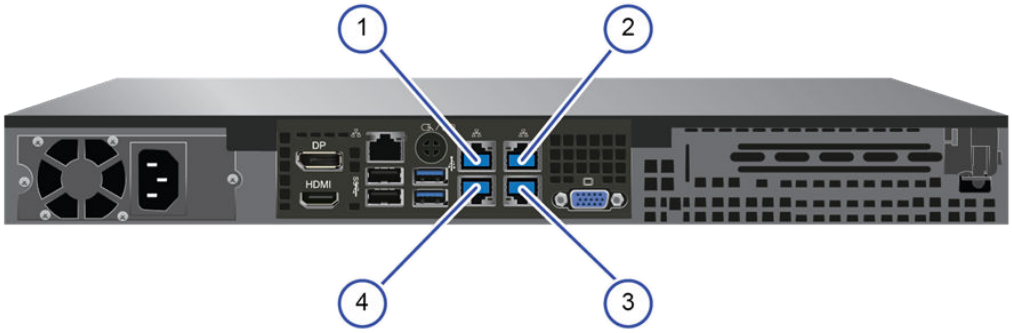


Table 2 SVP (Windows 10 Enterprise) rear panel

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

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: The SVP's default MTU size is 1500.

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 3: 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 (Windows 7) front panel

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

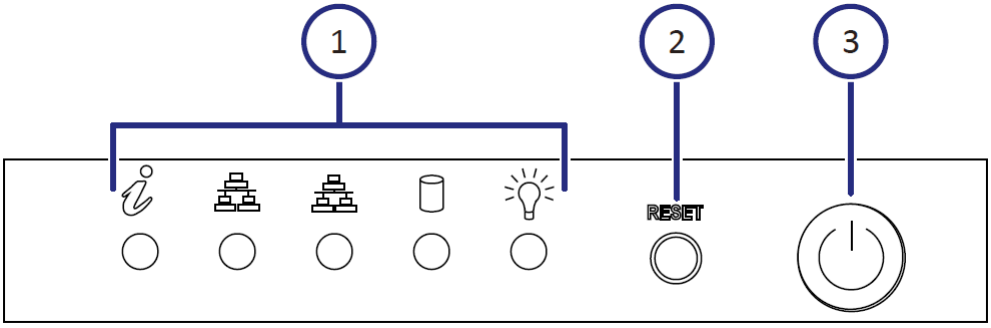


Table 3 SVP (Windows 7) front panel

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 (Windows 7) 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.

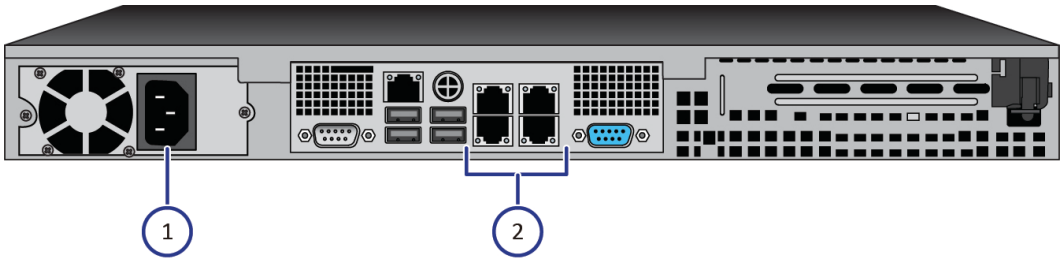


Table 4 SVP (Windows 7) rear panel

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.

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.

Note: The SVP's default MTU size is 1500.

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 4: Installing the Hitachi Vantara-supplied SVP

Hitachi Vantara provides a 1U SVP for use with VSP Gx00 models, VSP Nx00, 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.

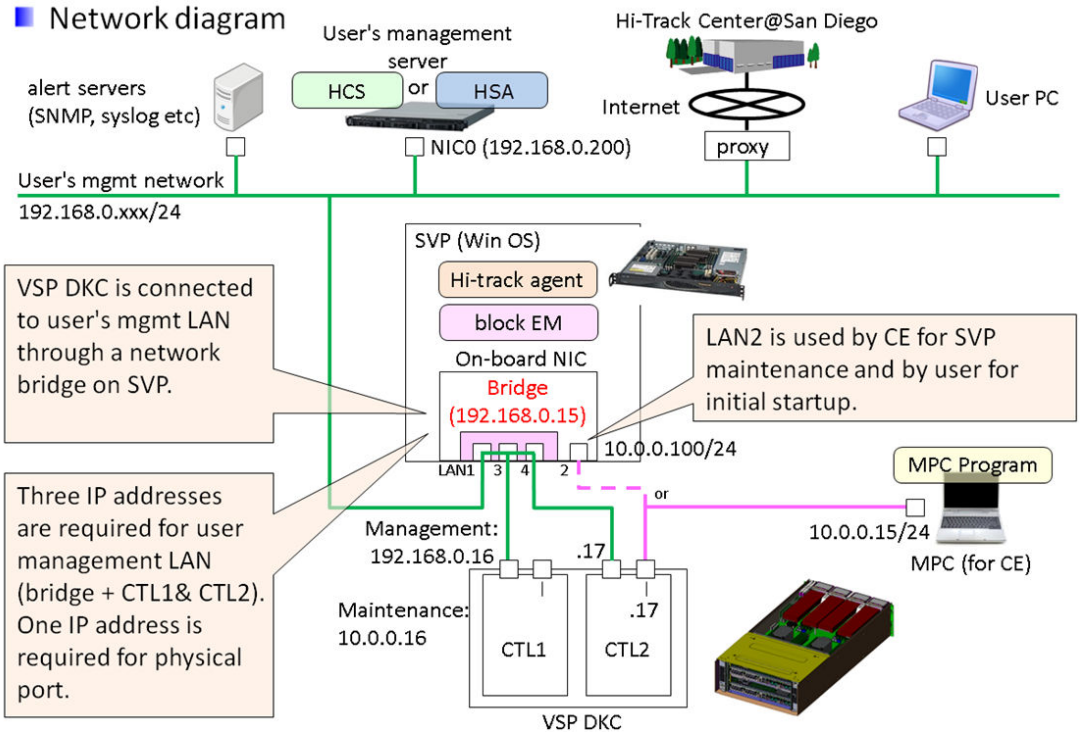
Important: The Hitachi Vantara-supplied SVP can only be installed, upgraded, or replaced by a Hitachi Vantara representative or an authorized service provider. Contact a Hitachi Vantara representative for more information about installing, upgrading, or replacing a Hitachi Vantara-supplied SVP.

Physical SVP network configuration

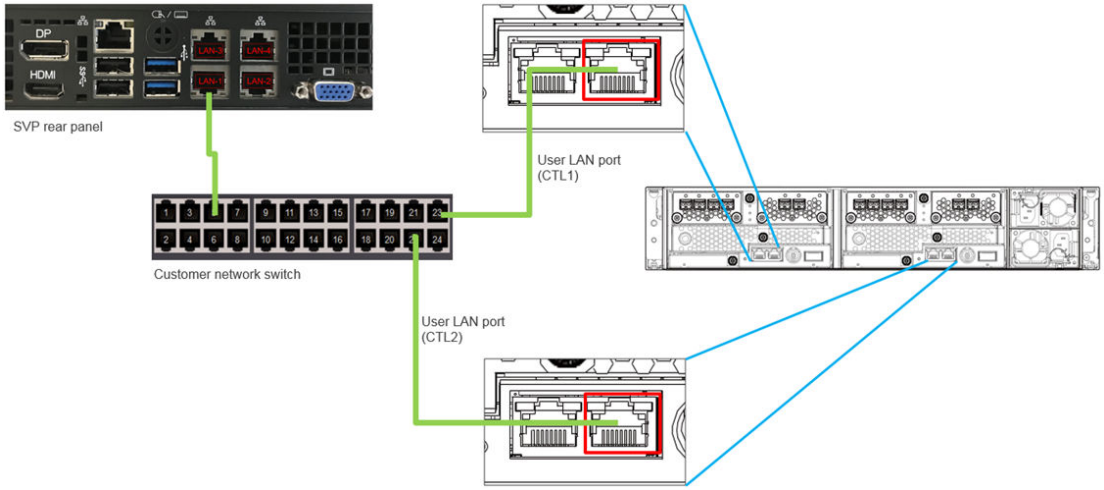
In networking terms, a *network bridge* is software or hardware that connects two or more networks so that they can communicate. For the physical SVP, a network bridge configures the three local-area network (LAN) ports on the SVP using the Bridge Connections setting in the Windows operating system.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



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

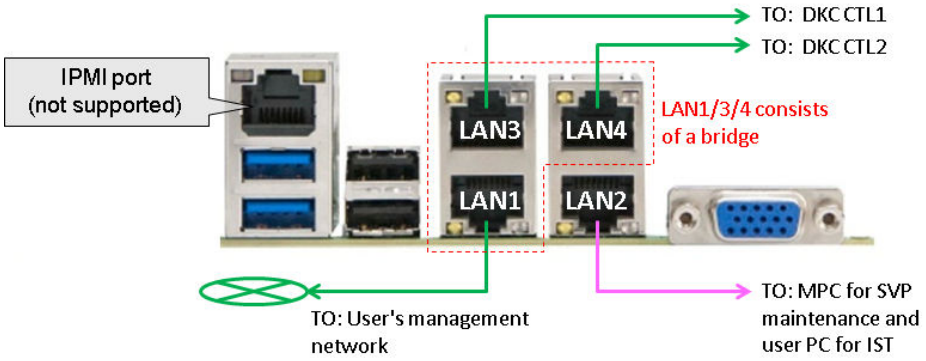


For information about configuring an SVP for a non-bridged network environment, see Operating the physical SVP in a non-bridged network configuration (on page 31) .

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.



Default IP address settings

The physical SVP is pre-configured with a default IP for the LAN 1/3/4 ports.

The user connects to the SVP using the IP address 192.168.0.15 for the 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

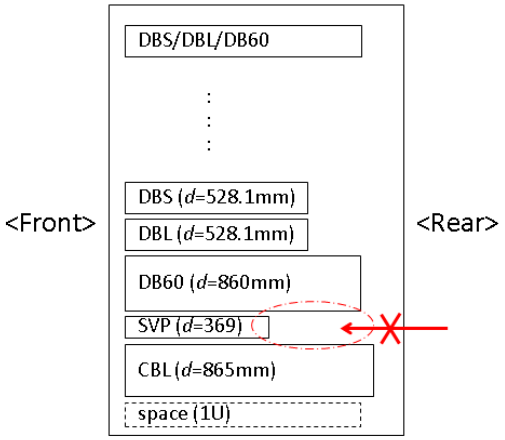
The following describes how to install the physical SVP into a rack and configure it for your network environment.

> **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). 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.

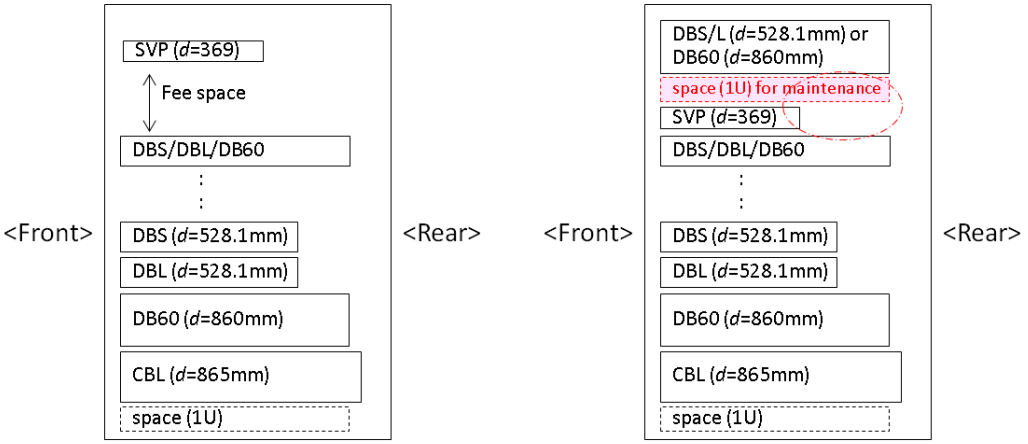


a) Bad example of rack-mounting with SVP

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.

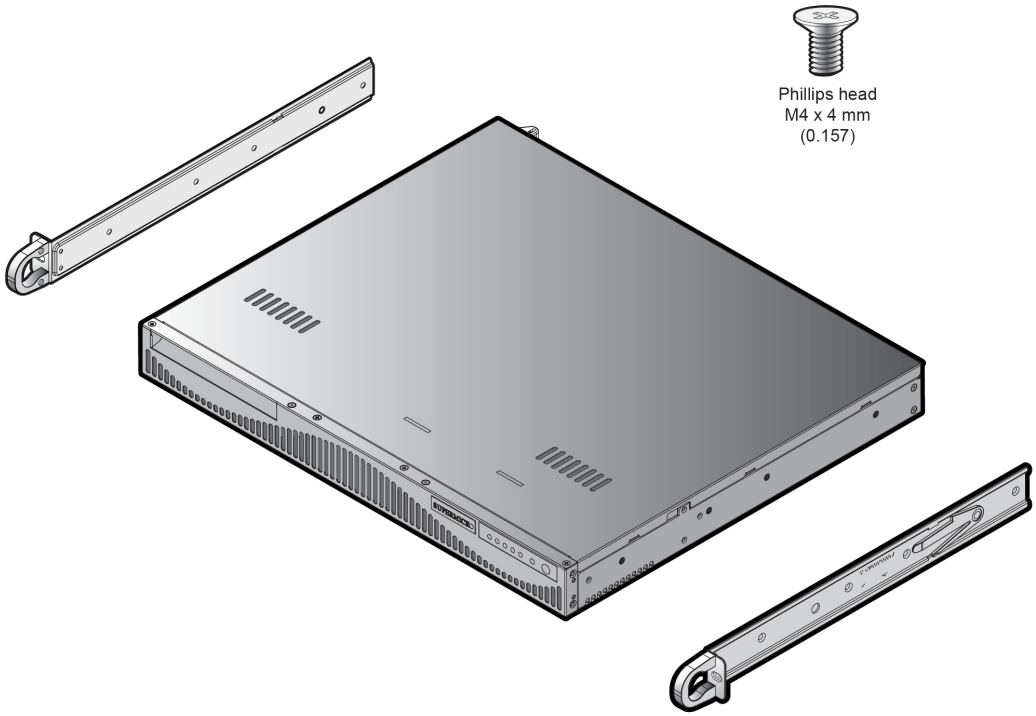
Installing the inner rail extension

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.

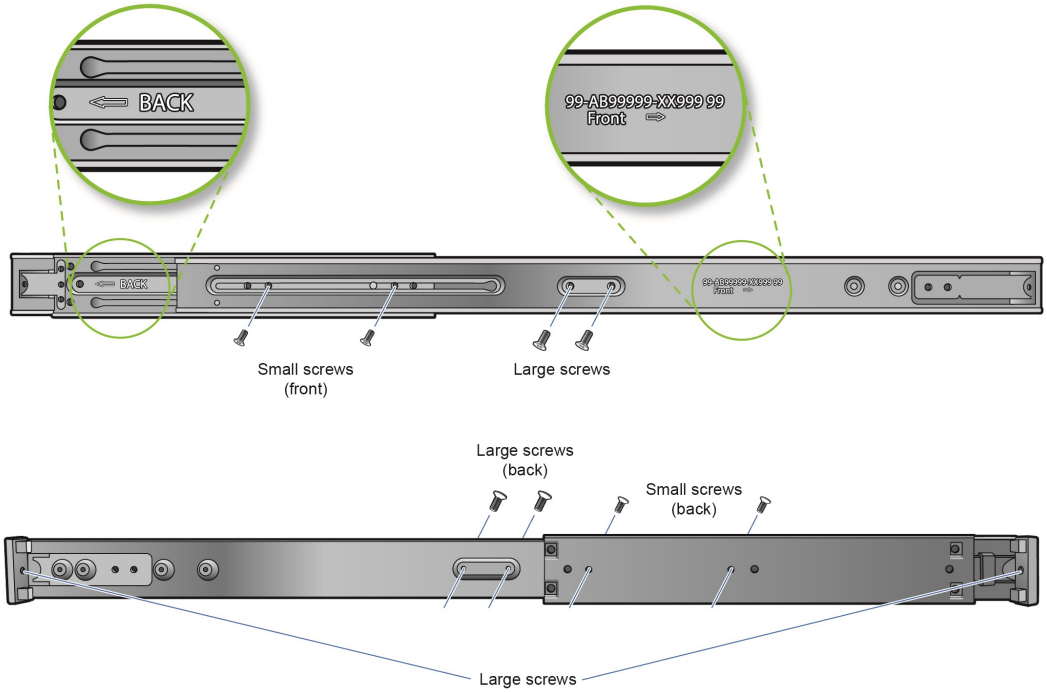
Installing the outer rails to the rack

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:

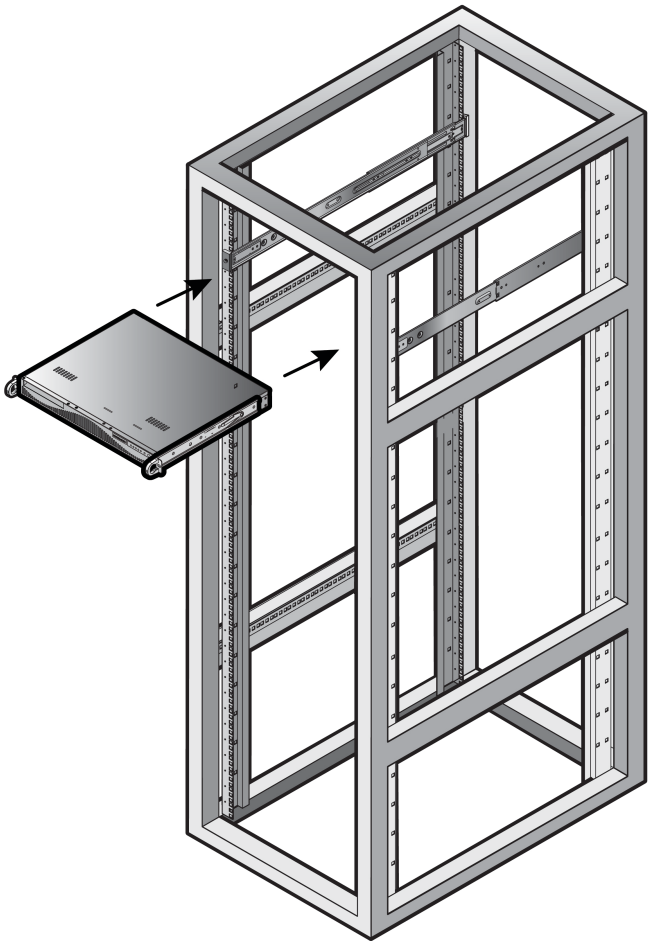
- The inner rails are attached to the SVP enclosure.
- The outer rails are attached to the rack.

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.

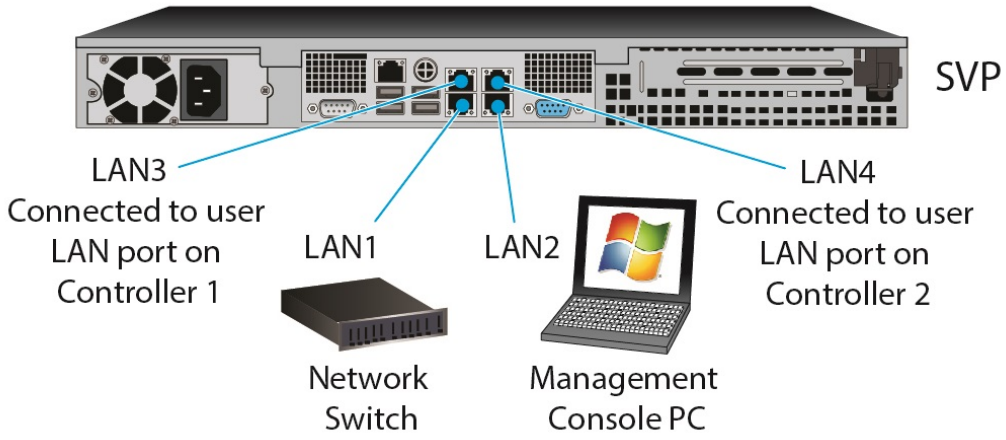
Procedure

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.

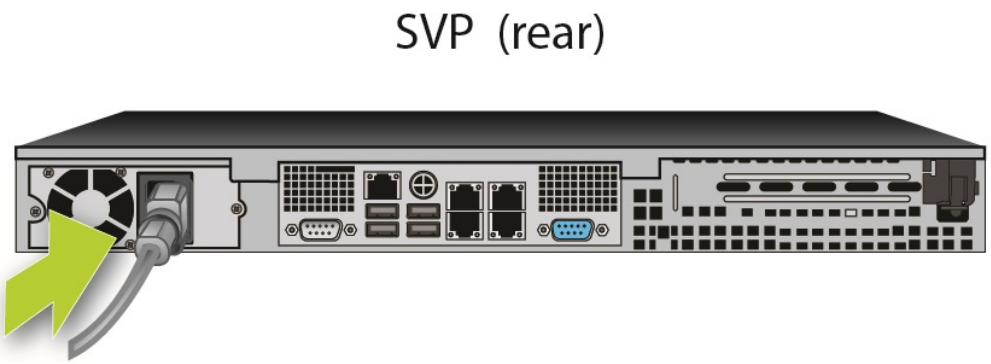
Note: Creating private and public keys requires a dedicated program, OpenSSL. OpenSSL is installed along with Storage Navigator but not allowed to be used for different purposes. To use OpenSSL for SSL communication settings, download one from the OpenSSL website (http://www.openssl.org/).

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

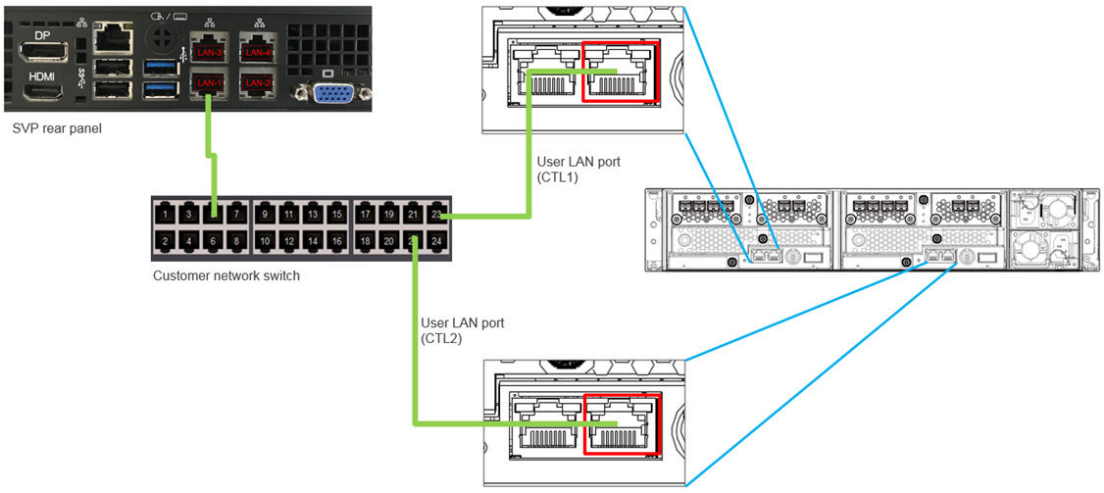
If Bridge Protocol Data Unit is enabled in your network environment, use a non-bridged configuration. This configuration disables the SVP's internal bridge, and allows you to connect the Ethernet cables from the user LAN port on CTL1 and CTL2 to an Ethernet switch.

Procedure

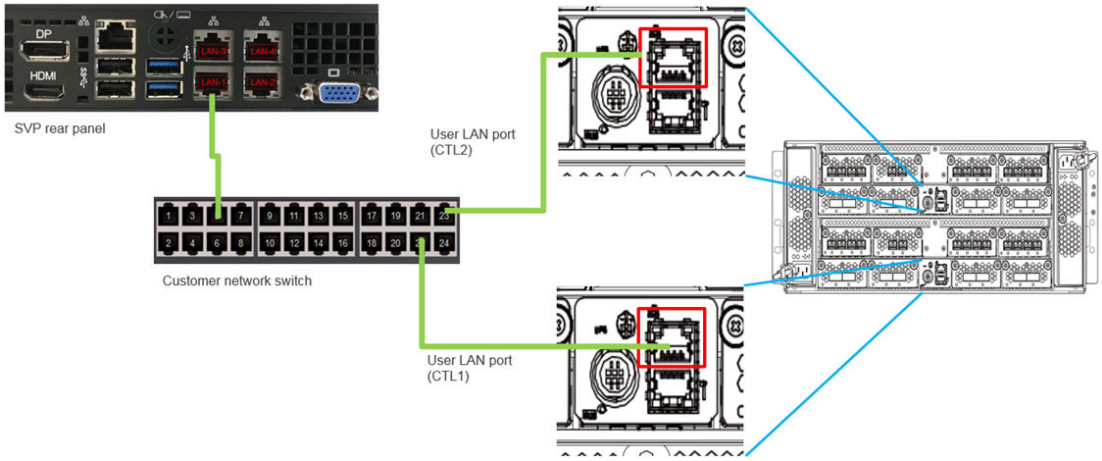
1. Connect a PC to the LAN2 port on the SVP.
2. Log on to the SVP using the Remote Desktop Connection:
   a. Configure the PC to use an IP address of 10.0.0.xxx, where xxx = 1-99 or 101-254, and a subnet mask of 255.255.255.0.
   b. Click **Start** > **All Programs**, and then select **Accessories** > **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.

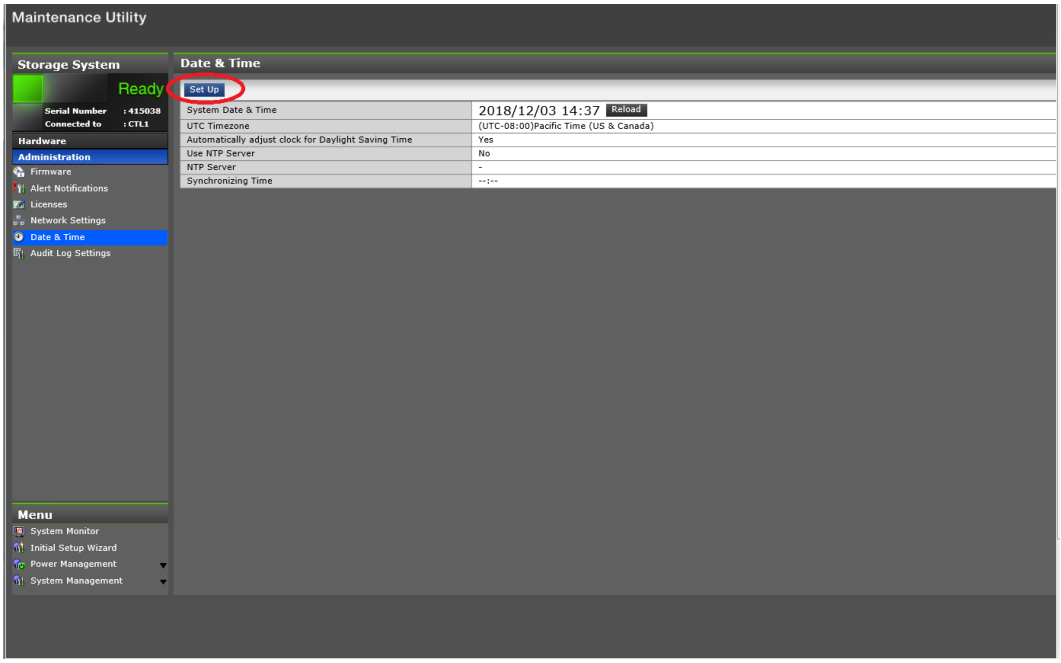
Before you begin

- 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.

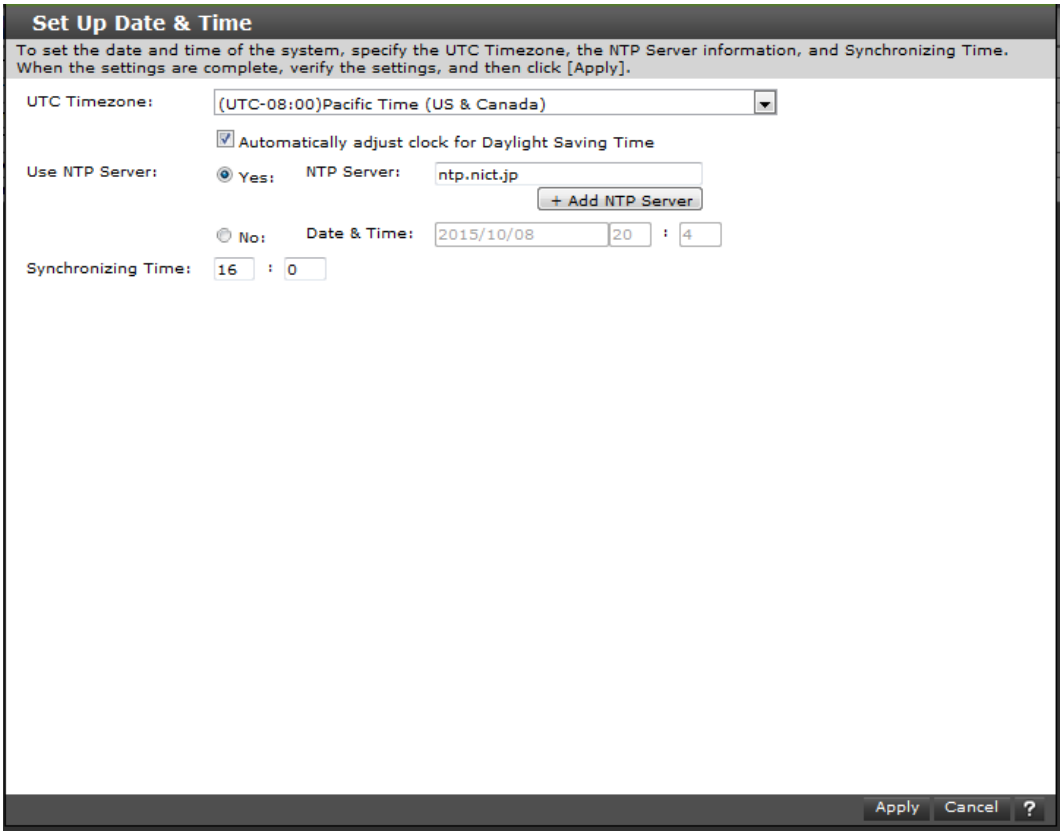
Procedure

1. Using the Windows operating system on the SVP, change the year, month, day, time, and UTC timezone according to the location in which the installed SVP resides. For more information, refer to your Windows documentation.

2. Log on to Hitachi Device Manager - Storage Navigator.
3. In the menu bar, click **Maintenance Utility** > **Date & Time**.
4. On the right side of the page, under **Date & Time**, click **Set Up**.



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



Field	Description	
UTC Time zone	Select a time zone on the Coordinated Universal Time map.	
Automatically adjust clock for Daylight Saving Time	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).	
Use NTP Server	Select an option for maintaining the maintenance utility time.	
	Yes: NTP Server	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: !"#$ %&'()*+,/;<=>? @[\]^`{|}
	No: Date & Time	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.
Synchronizing Time	To synchronize the maintenance utility time with the NTP server at a specific time, enter the synchronizing time.	

6. Click **Apply**.
7. 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, VSP Nx00, 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.

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) .

Prior to installing the SVP software, use the Remote Desktop Connection to log on to the SVP as the user who was specified during the Windows installation (for example, `Administrator`). After logging on, configure the Windows operating system on the customer-supplied server. Most of these settings can be configured using the Windows Control Panel. For detailed information about configuring these settings, refer to the documentation for your Windows operating system.

Note: These procedures assume that the operating system has already been installed on the server.

SVP locale

- The SVP and storage management software support the English and Japanese languages.
- To install the SVP software using a language other than English and Japanese, change the SVP's locale setting to reflect the appropriate language.

Desktop icons

- Configure the desktop for large icons.

Desktop configuration

- Set the screen saver to blank.
- Set the wait time to 60 minutes.

Taskbar and Start menu properties

- Always show all icons and notifications on the taskbar.
- Open the **Taskbar and Start Menu Properties** window. Click Customize in the **Start Menu** tab. Check Run Command and Display on the All Programs menu and the Start menu. Under Music, check Don’t display this item.

Time settings

- Configure the SVP for Universal Coordinated Time.
- Configure the SVP to not synchronize with an Internet time server.

Region settings

- Hide the language bar.
- Using System Locale, select the language for your region or preference, and then restart the server.
- In the Text Services and Input Language box, check whether Japanese(Japan) appears under Installed services. If it does, click the current selection, and then click Remove.

Power management settings

- Configure the high-performance power options to never turn off the display.
- Change the advanced power settings to never turn off the hard disk.
- Set the Minimum processor state percentage to 5.

Change Action Center settings

- Clear all items in the **Change Action Center** window.

Troubleshooting settings

- In the **Change settings** window, set Computer Maintenance to Off, and clear all configuration options below Other settings.

Remote Desktop settings

- Clear Allow Remote Assistance connections to this computer and check Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure).
- Select Remote Desktop and Remote Desktop - RemoteFX for both Home/Work (Private) and Public.

Internet Explorer settings

- Select Allow active content to run in files on My Computer.
- Clear SSL 2.0 and select Use TLS 1.2.
- In the **Turn on Suggested Sites** window, click No, don't turn on, and then click Next. In the **Choose your settings** window, click Use express settings, and then click Auto-execute settings

  Finish.
- Turn off the Windows AutoPlay feature.
- In the **Property** window, click Enabled and select All drives, and then click `OK`.
- Clear Use Autoplay for all media and devices.

Configure the Registry using Regedit

- Set HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control \Lsa > restrictanonymousto 1 and confirm that Hexadecimal is selected.
- Go to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server. In the Edit menu, click New > DWORD (32-bit) Value. Type `DisableBeep`, and then double-click it and set the value to 1. Confirm that Hexadecimal is selected.
- Go to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Terminal Services. In the Edit menu, click New > DWORD (32-bit) Value. Type `fPromptForPassword`, and then double-click it and set the value to 1. Confirm that Hexadecimal is selected.
- In the Edit menu, click New > DWORD (32-bit) Value. Type `SecurityLayer`.
- Restart the server.

ICMP reply settings. Click 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)

Computer name

- Change the computer name to `SVP-PC`.

Note: The computer name, `SVP-PC`, can be changed either before or after initial configuration.

Account name

- Change the account name to `SVP`. Then open the **Local Users and Groups** window and rename the user to `SVP`.

Password settings

- Change the Windows administrator password to `raid-login`.
- Change the password for the Windows operating system running on the SVP to `raid-login`.

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

- Open and expand Internet Information Services, and then 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
- Uncheck World Wide Web Services.

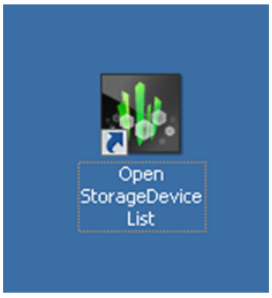
Installing the SVP software

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`**.

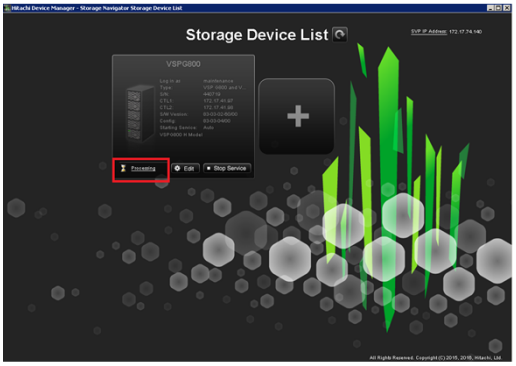
Procedure

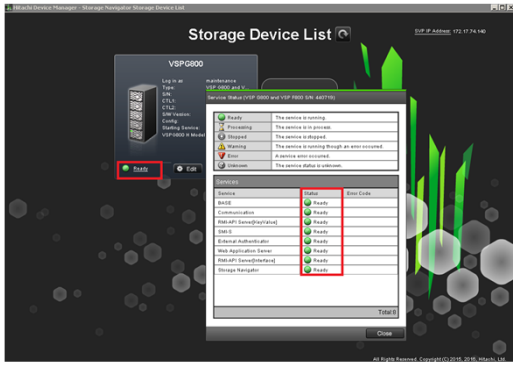
1. Obtain the appropriate SVP ISO image for your storage system from the firmware distribution set. Verify the ISO image corresponds to the firmware currently running on the storage system.
2. Download the SVP ISO from TISC to the CE notebook, and then use an ISO reader to mount the SVP ISO as the next 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 and click **Apply**.
11. Add the storage system.
12. Register the storage system.
13. 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
14. 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 Click **Apply**, and then click **Confirm** to added the storage system to the SVP.
15. On the Desktop, click the **Open StorageDevice List** shortcut.

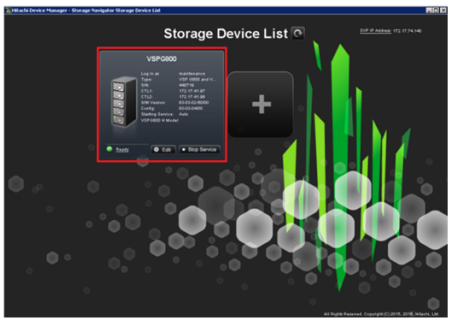


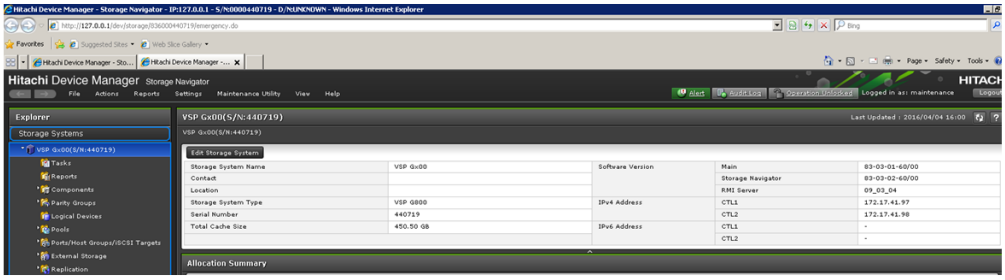
Wait 10-to-15 minutes for all the services to start.





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





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

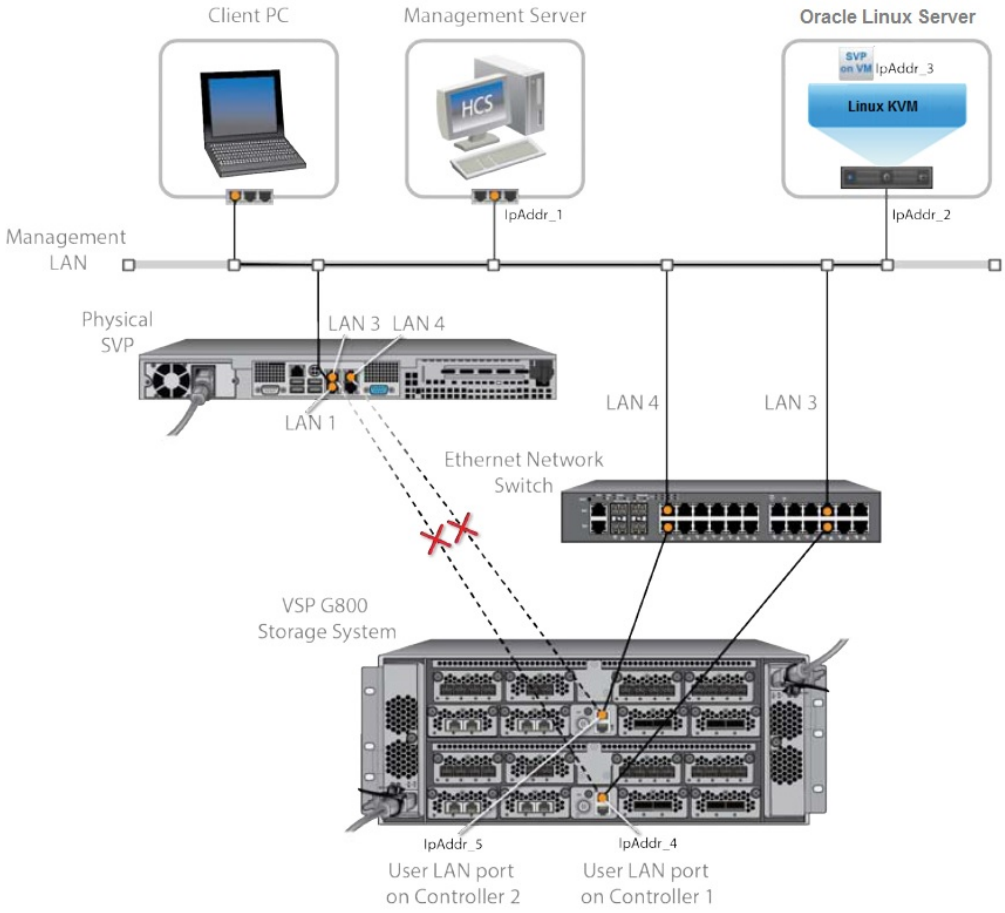
Hitachi Vantara supports configurations where a single SVP communicates with a single VSP Gx00, VSP Nx00, or VSP Fx00 model. This configuration can coexist with, or replace, all other physical, virtual, and bare-metal SVP configurations.

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, VSP Nx00 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)

For the latest interoperability updates and details, see https://support.hitachivantara.com/en/user/answers/interoperability.html.

Miscellaneous

- WinZip

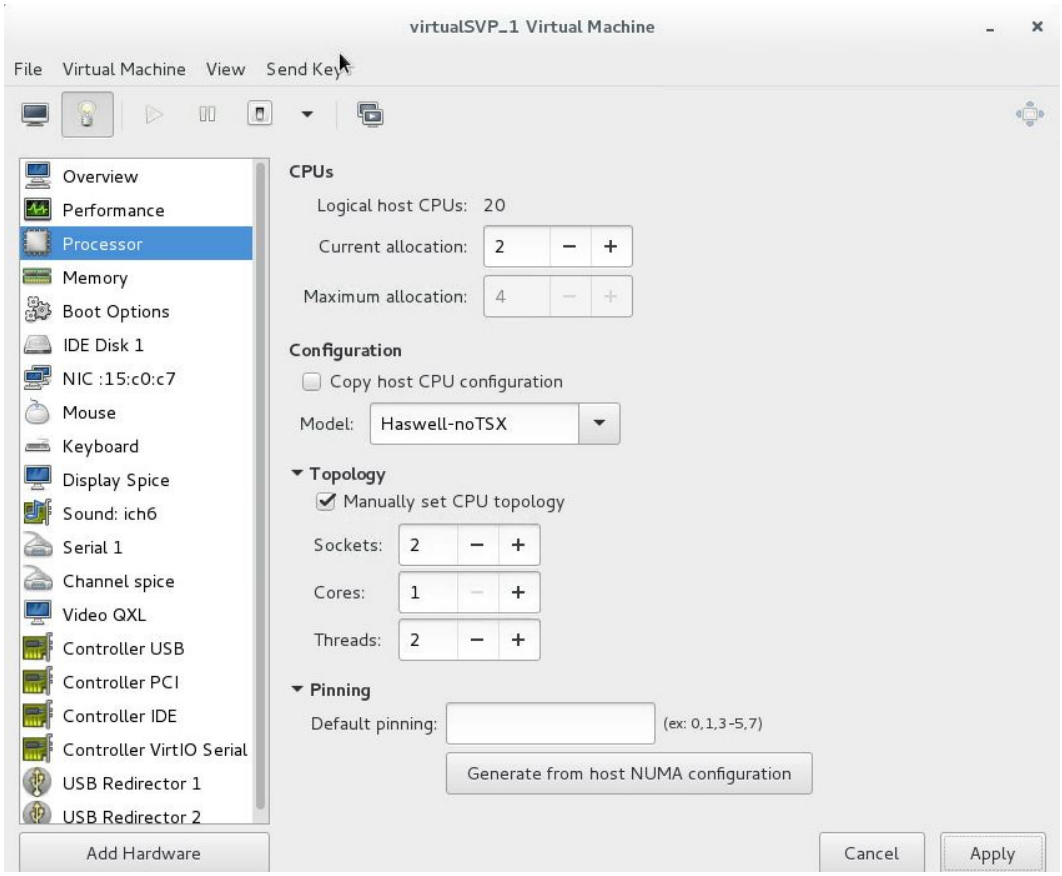
Hyper-threading

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.

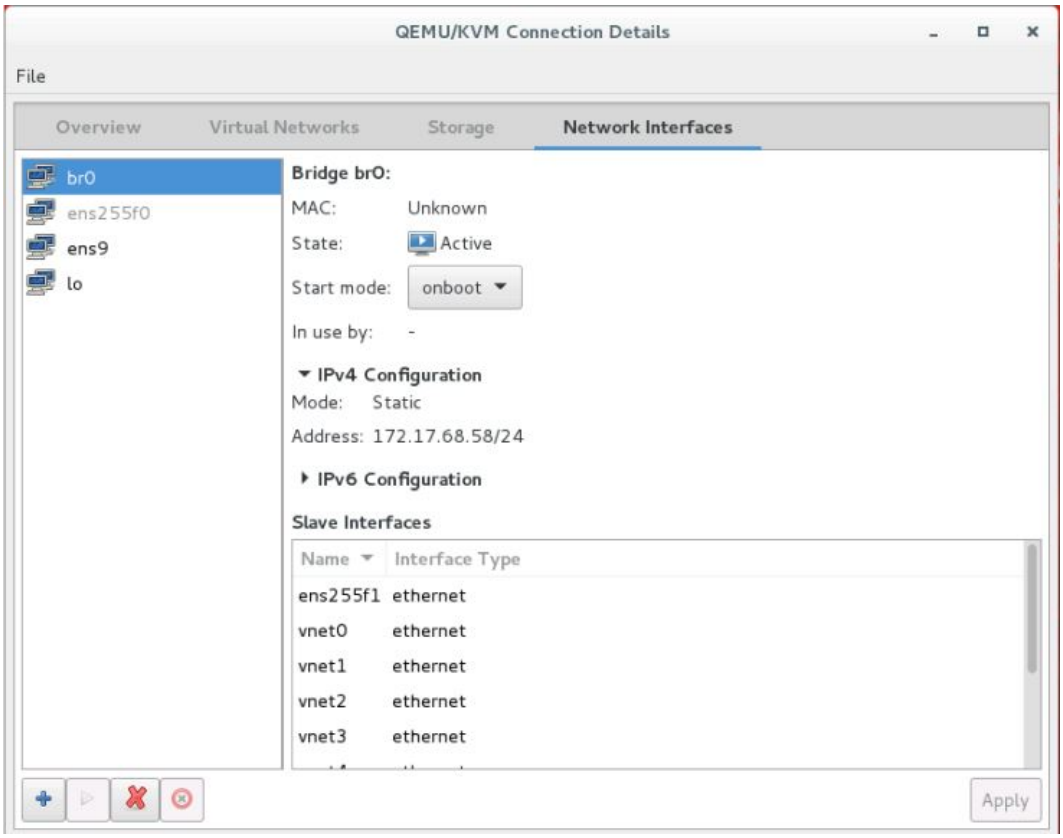


Configuring the Oracle Linux KVM-based SVP

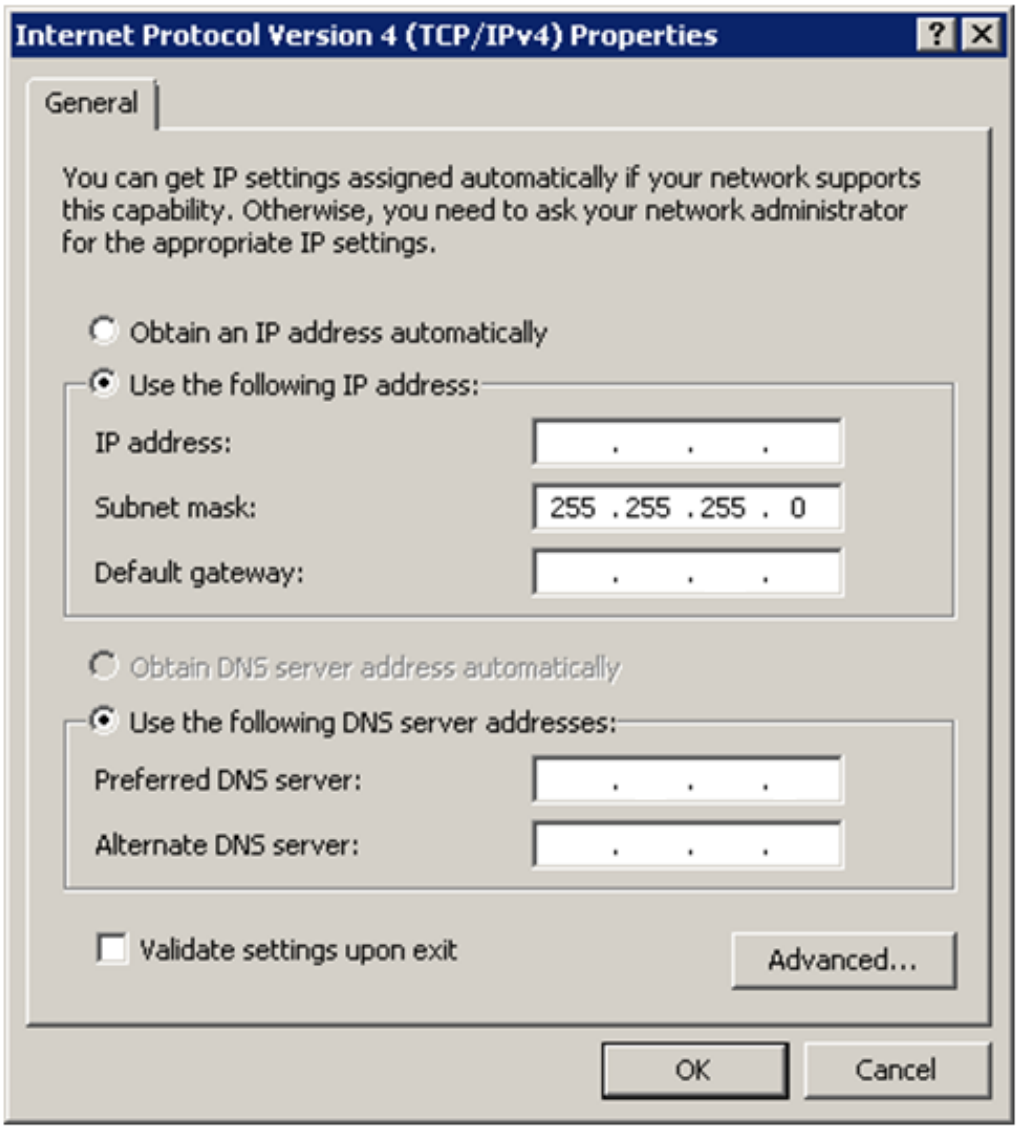
After preparing the environment, activating hyper-threading on both the Oracle Linux KVM server and VM guest host, and verifying the configuration layout, configure the SVP in the Oracle Linux KVM environment.

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.



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



4. Configure a Remote Desktop Connection.

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, VSP Nx00, 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

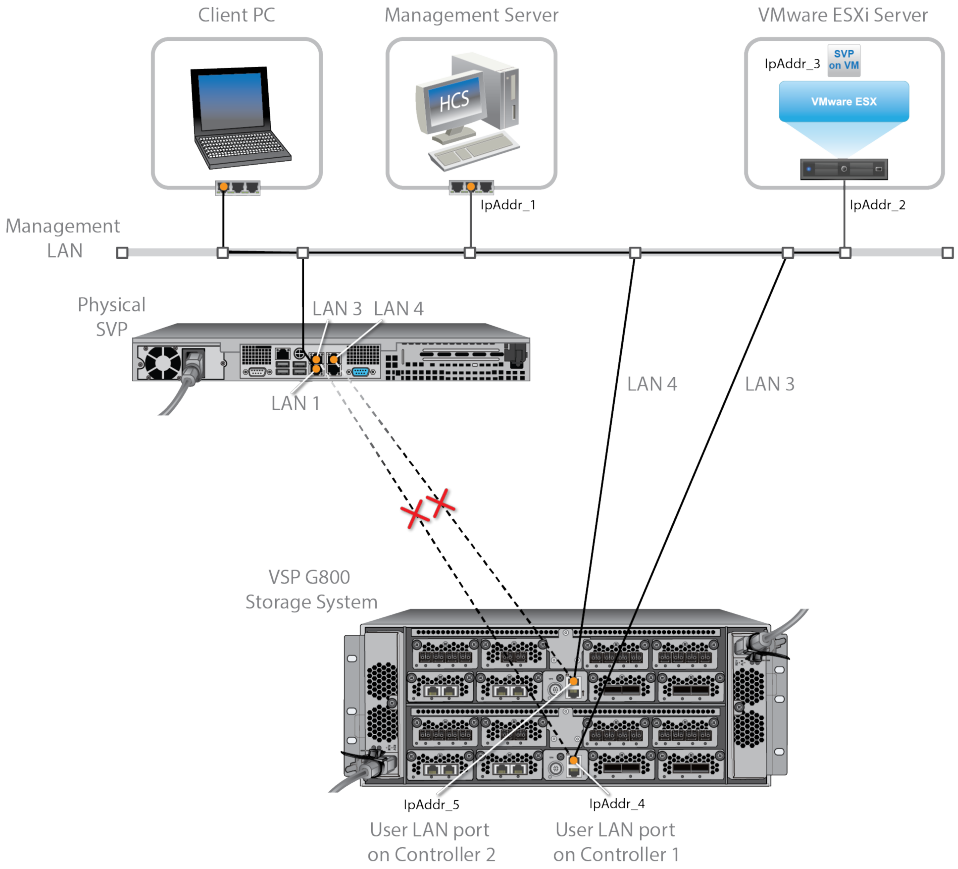
The SVP and storage management software support the English and Japanese languages.

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, VSP Nx00, 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)

For the latest interoperability updates and details, see https://support.hitachivantara.com/en/user/answers/interoperability.html.

Miscellaneous

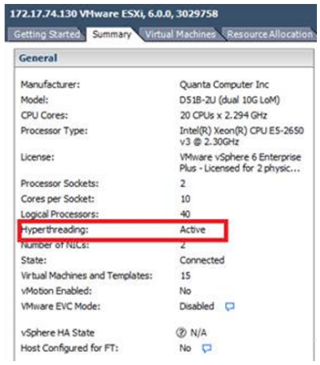
- WinZip

Hyper-threading

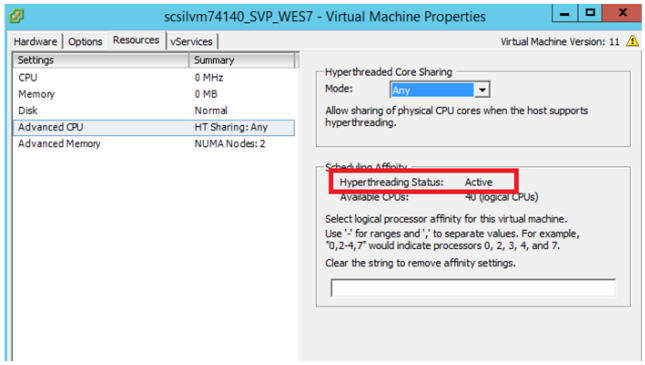
To support a virtual SVP, verify that hyper-threading is active for the ESXi server and VM guest host.

Note: Hyper-threading is enabled by default.

ESXi server



VM guest host

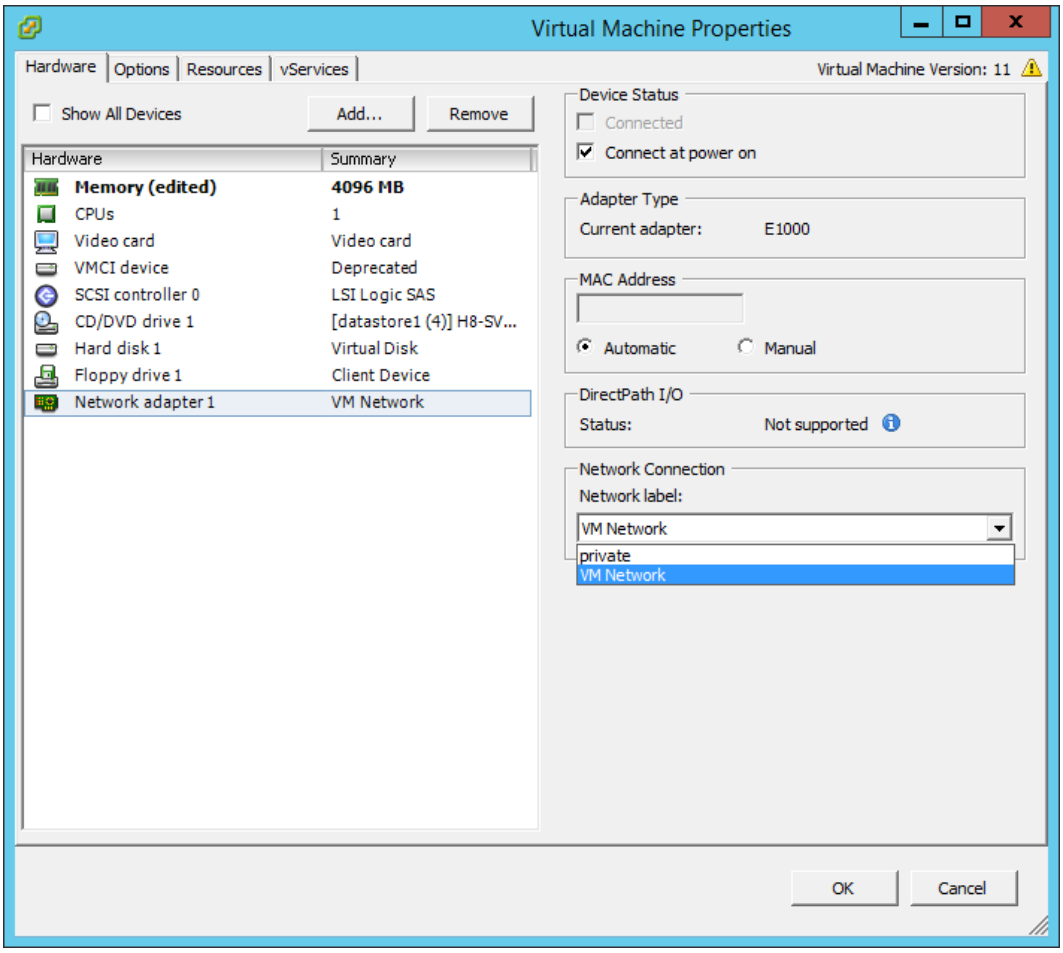


Configuring the virtual SVP

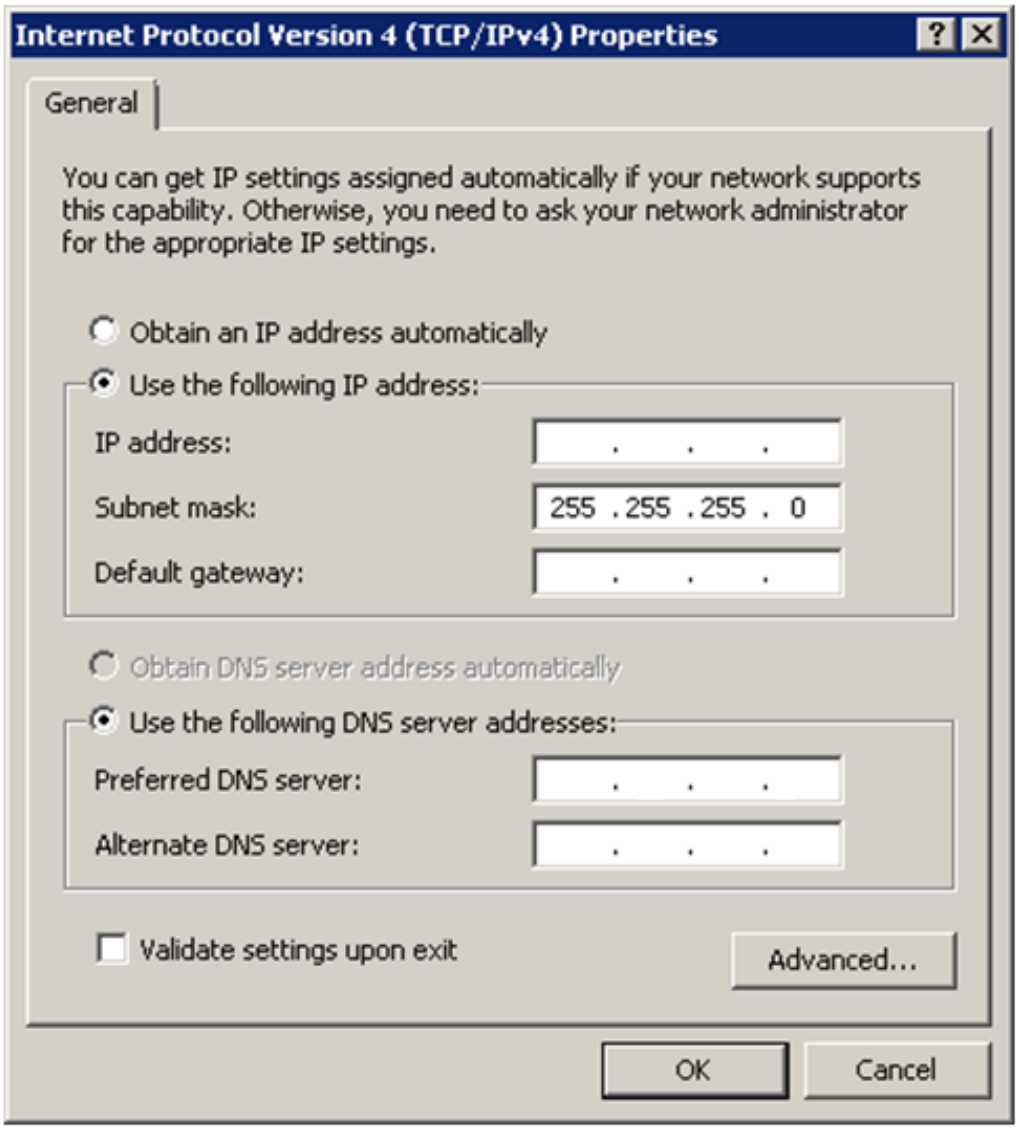
After preparing the environment, activating hyper-threading on both the ESXi server and VM guest host, and verifying the configuration layout, configure the virtual SVP.

Procedure

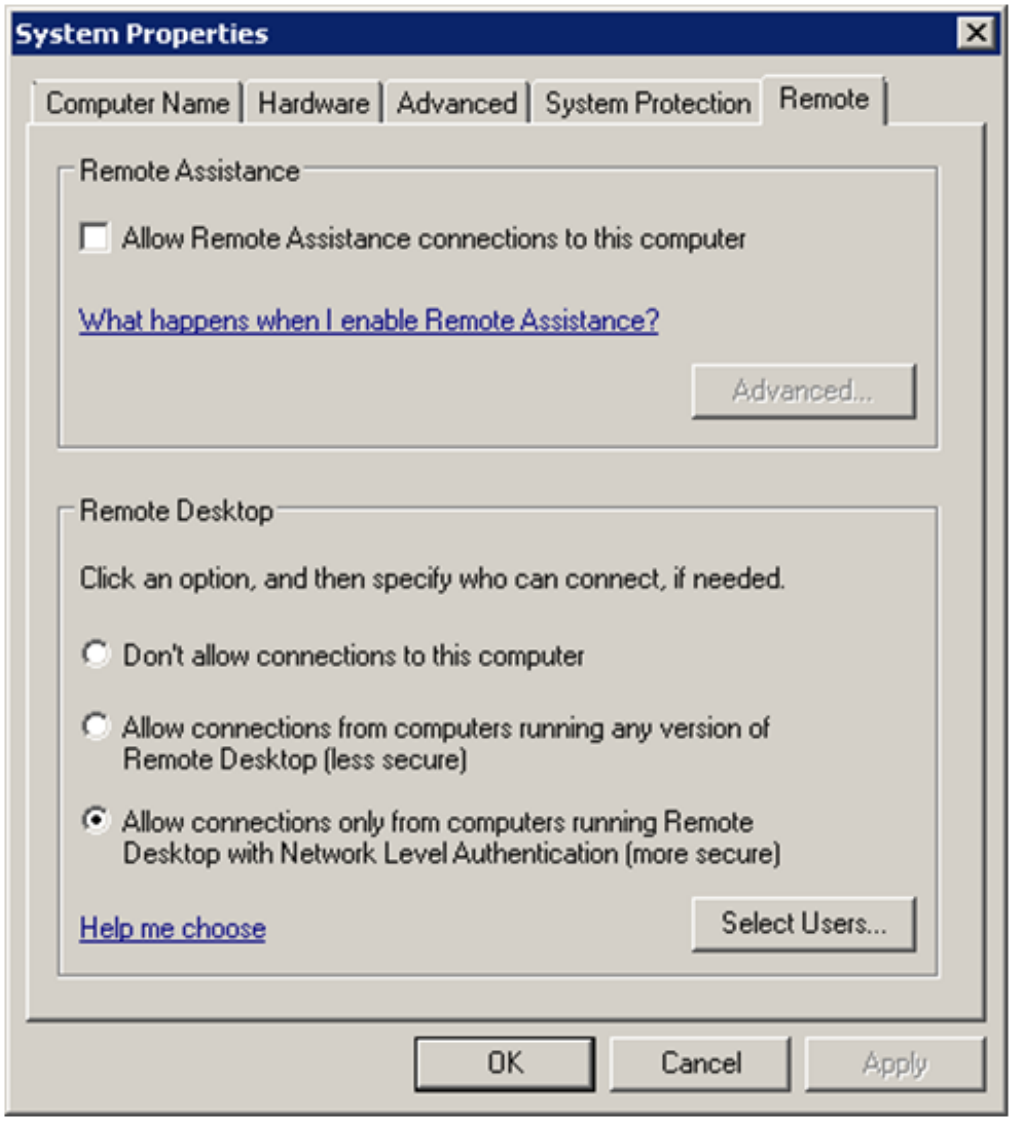
1. Create a Windows 7 Professional x64 Service Pack 1 environment on the ESXi host.
2. Verify the virtual network connection is properly assigned to the appropriate virtual machine network.



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



4. Configure a Remote Desktop connection.



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

Configuring the SVP guest OS

Before you begin, ensure Hyper-Threading is active for the ESXi server and VM guest host is configured.

For more information on configuring the operating system on the SVP, see Configuring the operating system (on page 36) .

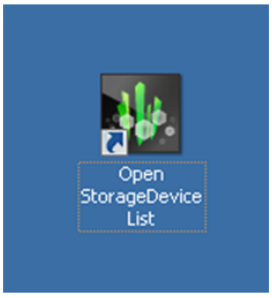
Installing the SVP software

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`**.

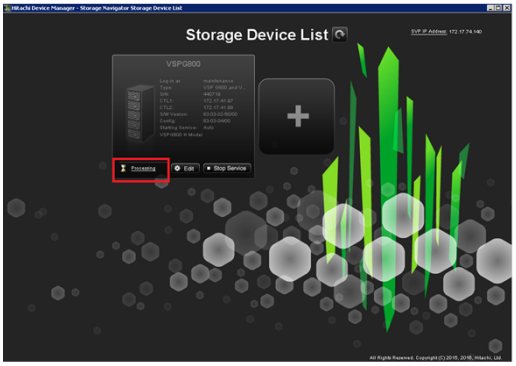
Procedure

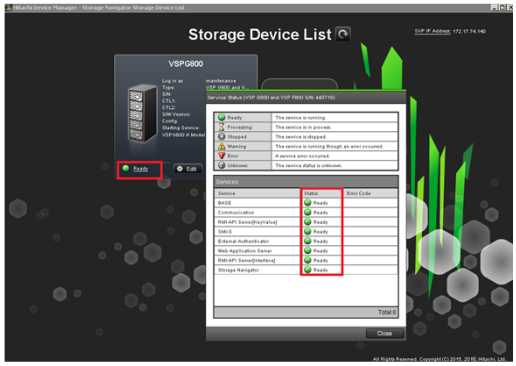
1. Obtain the appropriate SVP ISO image for your storage system from the firmware distribution set. Verify the ISO image corresponds to the firmware currently running on the storage system.
2. Download the SVP ISO from TISC to the CE notebook, and then use an ISO reader to mount the SVP ISO as the next 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 and click **Apply**.
11. Add the storage system.
12. Register the storage system.
13. 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
14. 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 Click **Apply**, and then click **Confirm** to added the storage system to the SVP.
15. On the Desktop, click the **Open StorageDevice List** shortcut.

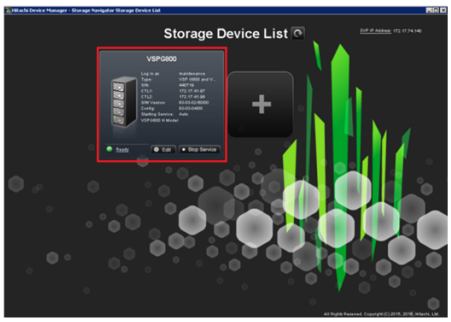


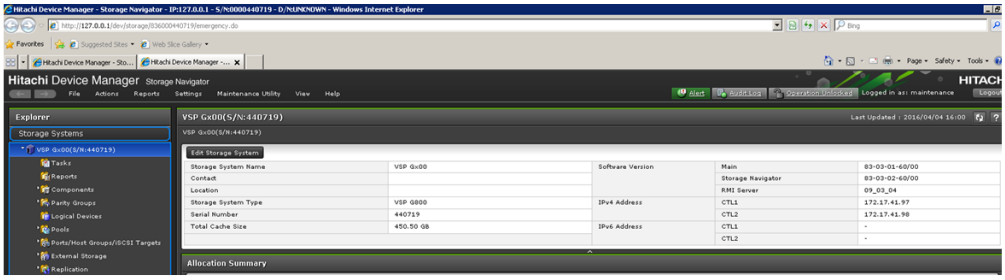
Wait 10-to-15 minutes for all the services to start.





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





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 50). 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 53).
   c. Install the SVP using the procedure in Completing the configuration (on page 40). 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
Hitachi Remote Ops	No report from the agent during a 24-hour health check	Remote Ops detects SVP failure -> SVP replacement. Contact a Hitachi Vantara representative or authorized service provider.
Hitachi Command Suite	RMI connection error (not alert)	See the *Hitachi Command Suite Administrator Guide* (MK-90HC175).
Hitachi Ops Center Administrator	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

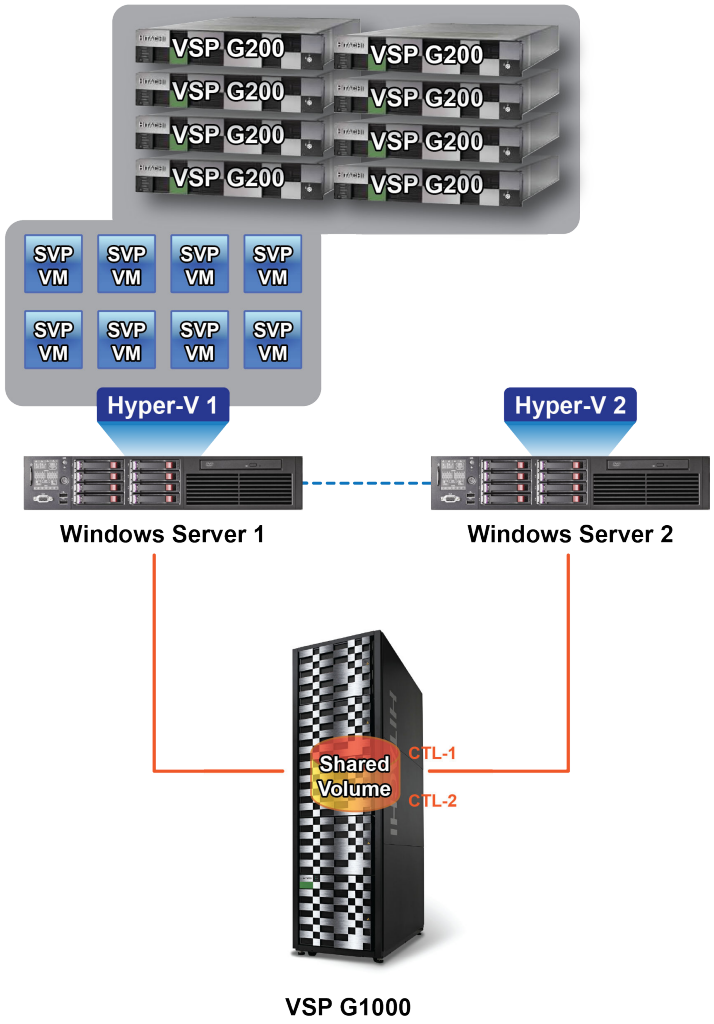
The SVP and storage management software support the English and Japanese languages.

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)

For the latest interoperability updates and details, see https://support.hitachivantara.com/en/user/answers/interoperability.html.

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.

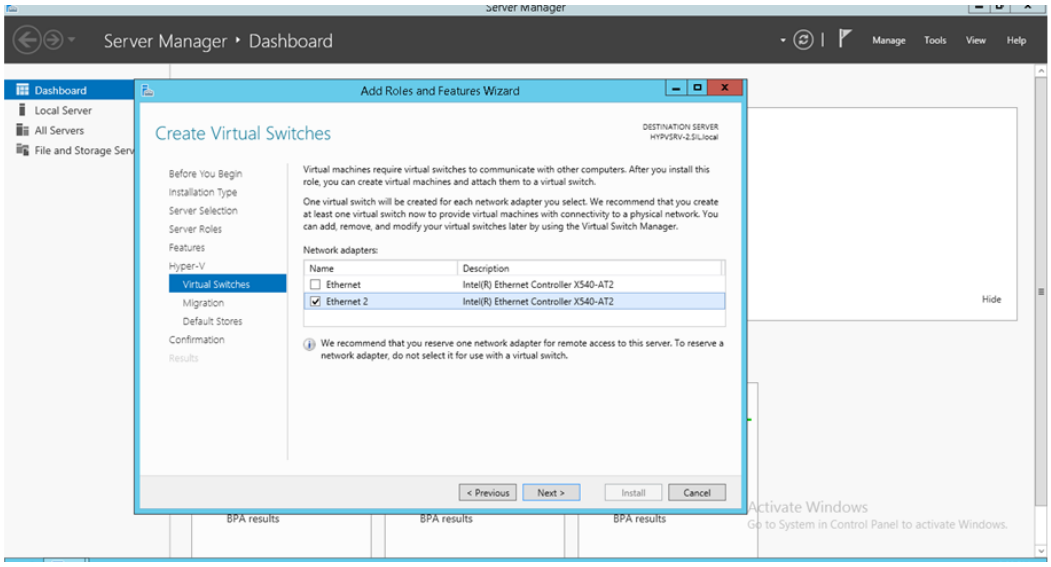
Installing and Configuring Hyper-V on Windows 2012 R2 Server

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.

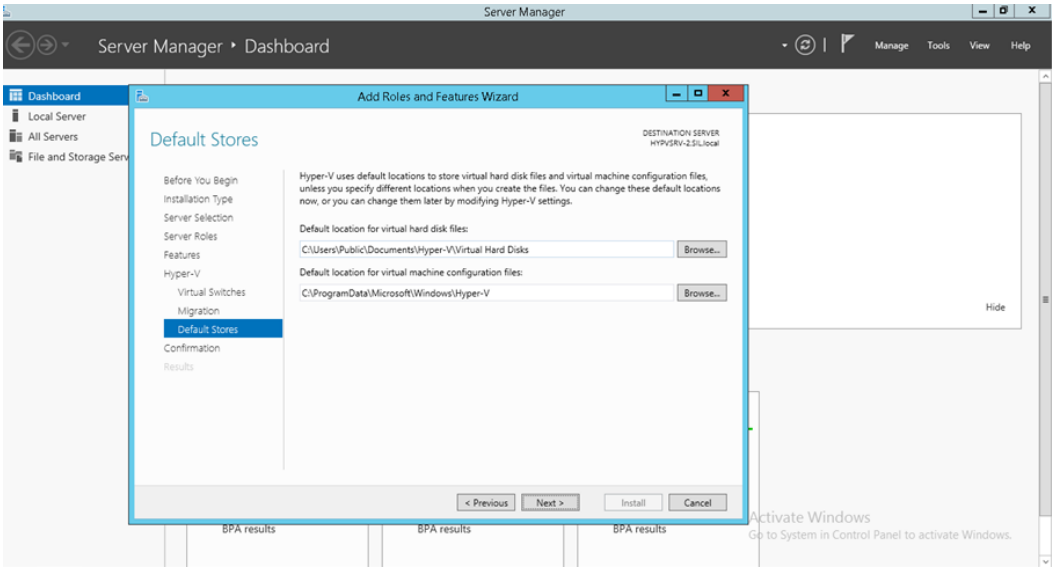
In the following procedure, you will define virtual switch settings. However, you will accept the default settings for the default stores; you can specify different locations later by modifying the Hyper-V settings.

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.



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.



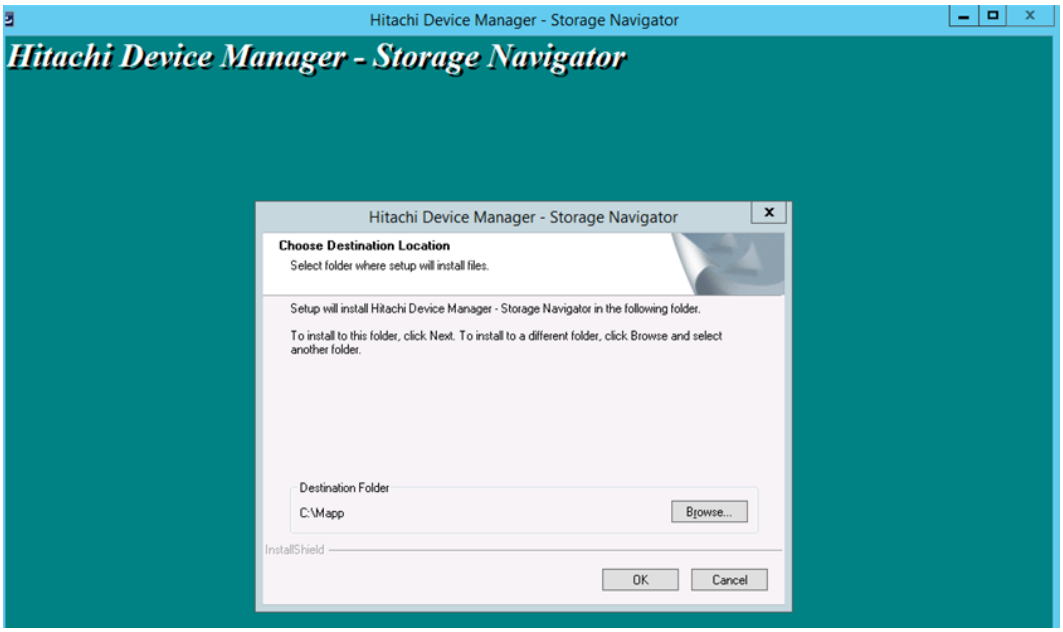
Installing the SVP software on a guest OS

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

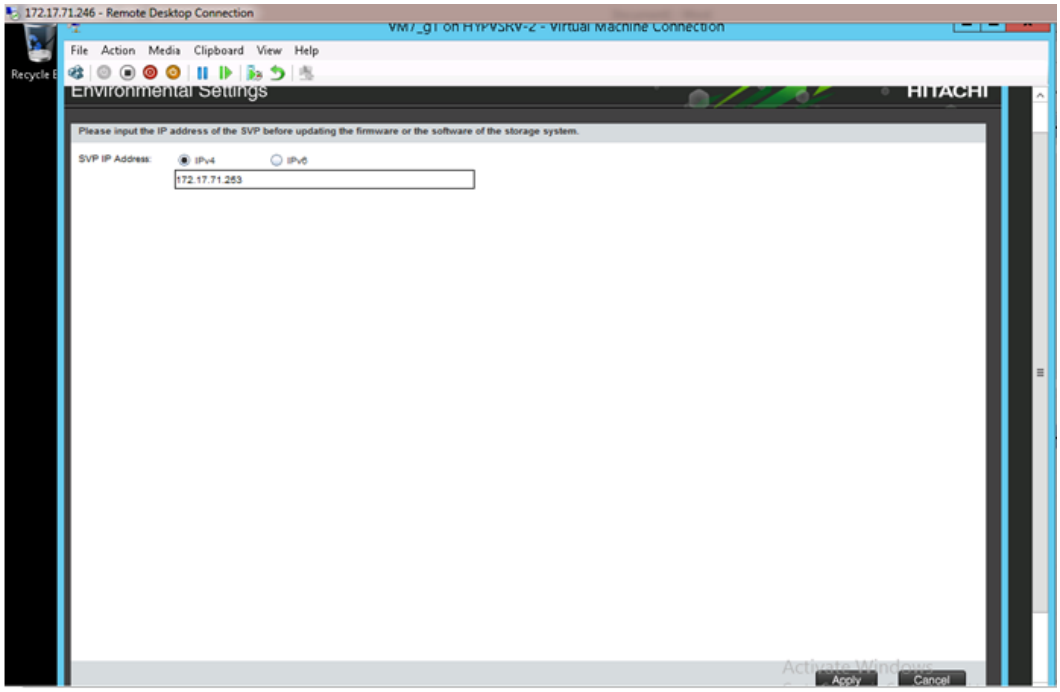
You install the SVP software using Hitachi Device Manager - Storage Navigator.

Procedure

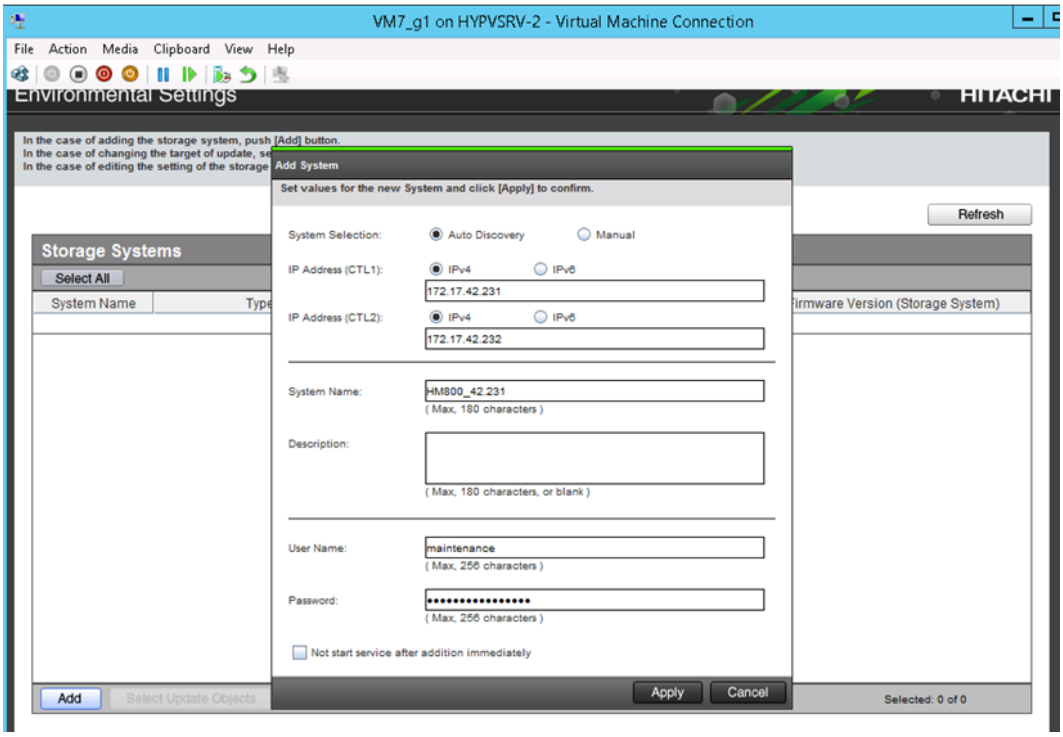
1. Double-click the `Setup.exe` file for Device Manager - Storage Navigator.
2. When prompted, select a language and accept the license agreement.
3. Accept the default directory or select a different one, and then click **OK**.



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**.



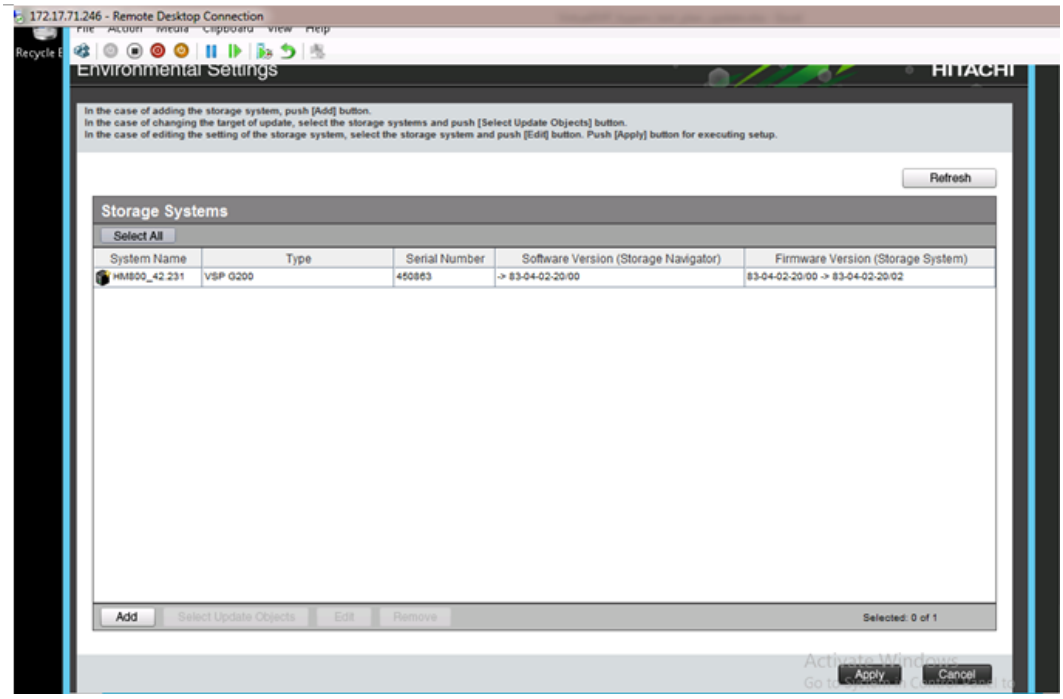
5. Complete the fields in the **Add System** window.



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 information manually. [1]
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.	

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



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

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

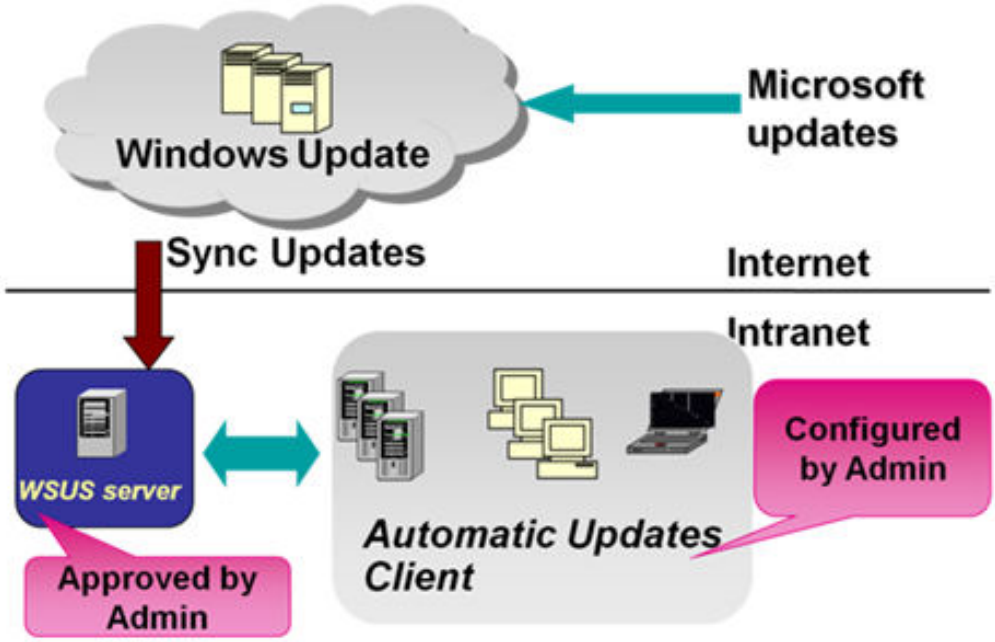
Only a Hitachi Vantara representative or authorized service provider can install, upgrade, and replace Hitachi Vantara physical and virtual SVPs. For more information, contact a Hitachi Vantara representative.

Chapter 10: Security patch and antivirus software

Windows and Antivirus Update Policies

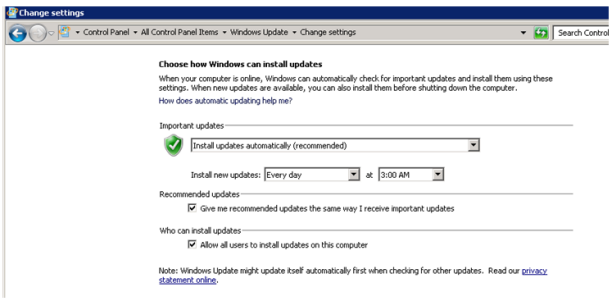
Use the SVP to provision storage, connect with other management software, execute scripts, or for maintenance purposes. An SVP is available as an option for the VSP E990 and the VSP G/F350, G/F370, G/F700, G/F900 models. An SVP is required for the VSP G200, G400, G600, G800, VSP F400, F600, F800, and VSP N400, N600, N800 models.

More importantly, Hitachi Vantara does not require access to the SVP. 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.

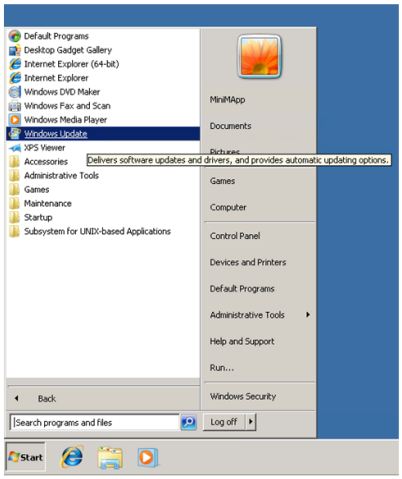


Online update

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



or



Offline update

You can apply appropriate Windows security patches by downloading stand-alone packages from the Microsoft Update Catalog.

When the catalog appears, use the Search field at the top right of the page to find security monthly rollups for Windows 7 or Windows 10, depending on the Windows operating system running on your SVP.

Tip: Create a restore point before installing a patch. That way, you have a way to back out of the patch if it causes issues after being installed.

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
- 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

For information about Windows 7 to Windows 10 upgrade path, contact customer support.

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.

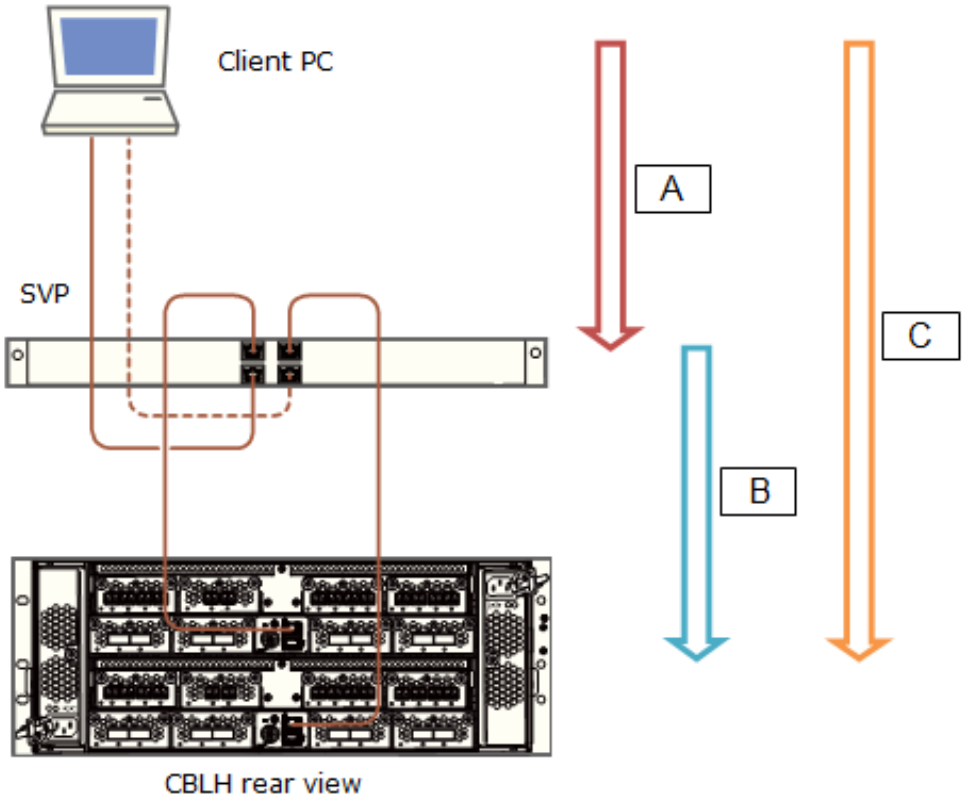
The following terms are associated with SSL:

- 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

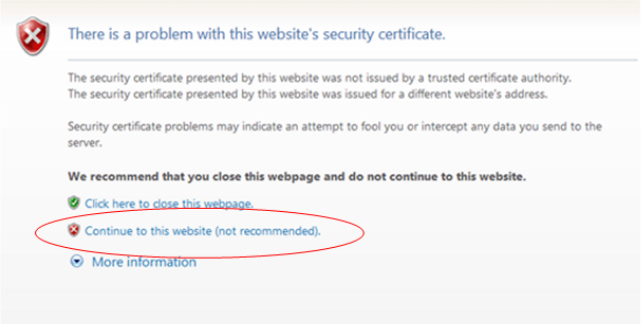
1. On the SVP, start a Windows command prompt as Administrator.
2. Move the current directory to the directory where the certificate update tool (`MappSn2GumSslCrtInit.bat`) is located. Issue the following command: `C:\MAPP\wk\Supervisor\MappIniSet\MappSn2GumSslCrtInit.bat`

> **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)**.



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.

   Note: Log on to the maintenance utility using a user account that has administrative privileges.

5. 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**.

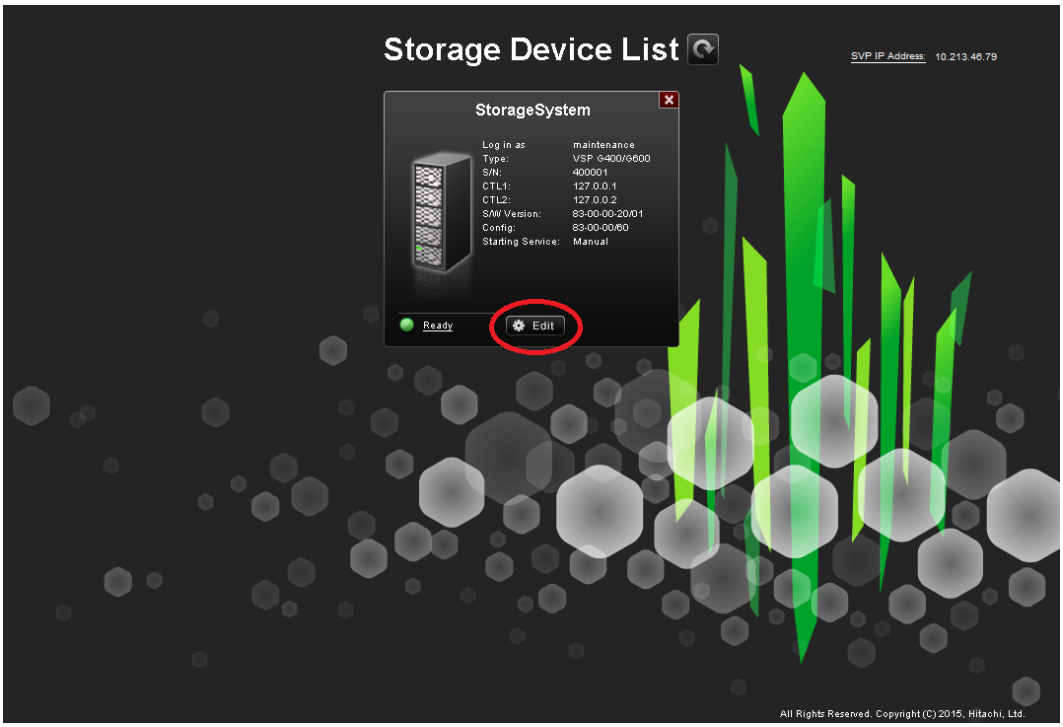
6. Set the user IP address.
   a. On the **Maintenance Utility** menu, click **Network Settings**.
   b. In the **Network Settings** window, click **Set Up Network Settings**.
   c. Set the IP address for controller 1 and controller 2.
   d. Click **Apply** and click **Log Out** to close the maintenance utility.
7. Change the storage system IP address in the **Storage Device List** window.
8. Set the SVP IP address.
9. Change the SVP IP address in the **Storage Device List**.
10. 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.

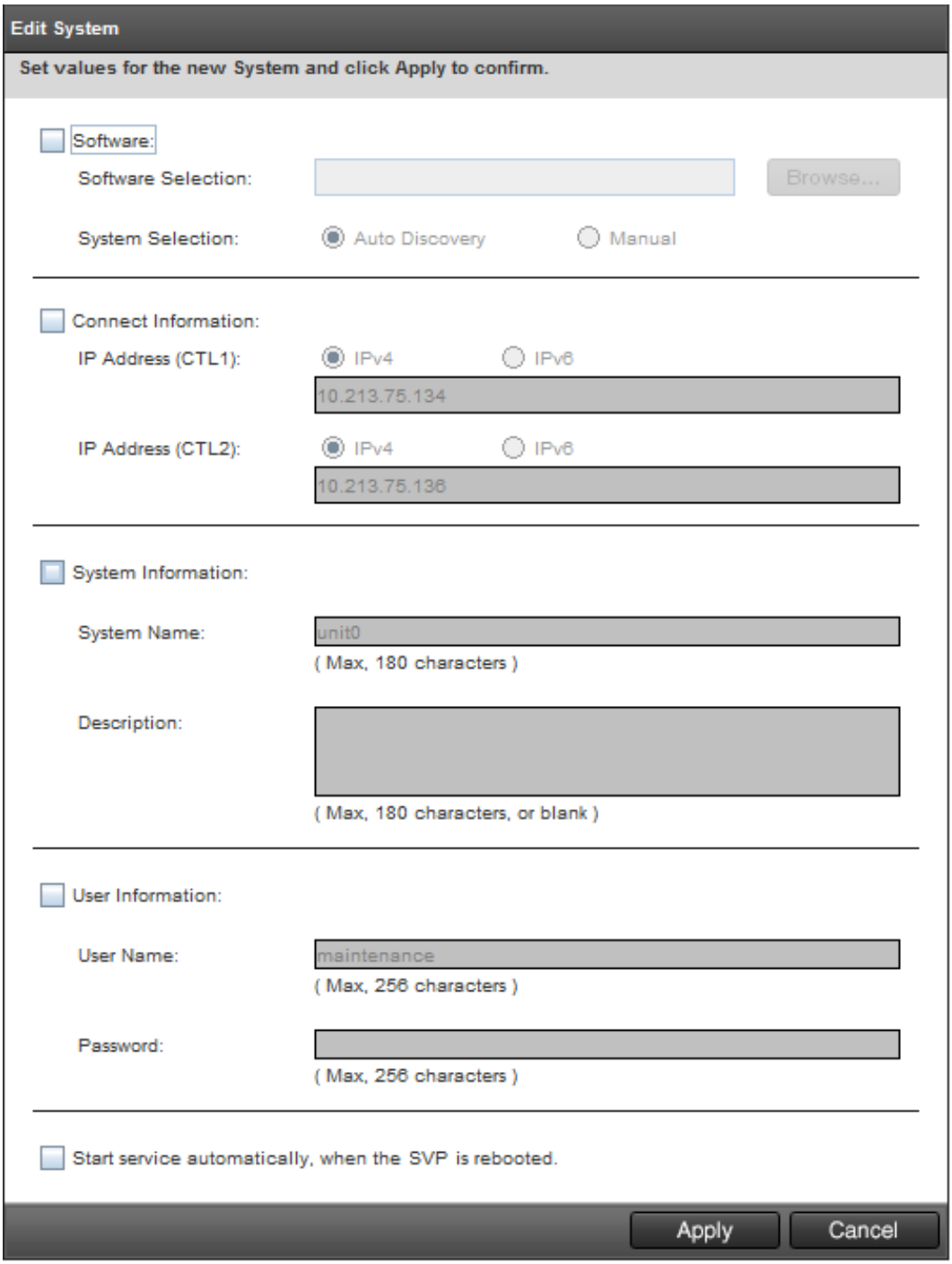
Changing storage system information in the Storage Device List

Procedure

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



The **Edit System** window opens.



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

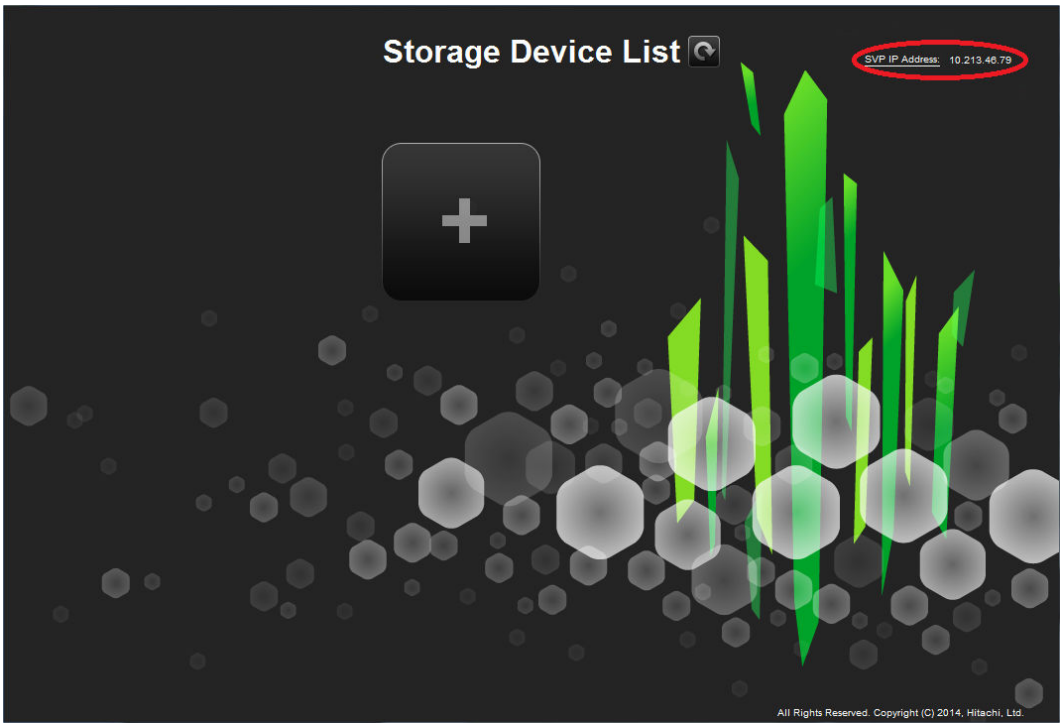
To change the SVP IP address in Storage Device List, change the IP address registered using the SVP's Windows operating system, and then perform the following procedure.

Before you begin

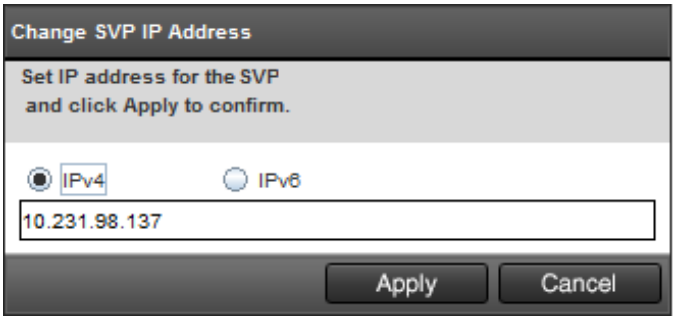
- Do not register the storage system on the SVP.
- Stop the service of the storage system.

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**.



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



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.

To change the range of the port numbers to be allocated automatically to a specific range of port numbers, see Changing range of port numbers to be allocated automatically (on page 95) and Reallocating automatically allocated port numbers (on page 93).

To initialize the range of port numbers to be allocated automatically, see Initializing range of port numbers to be allocated automatically (on page 97) and Reallocating automatically allocated port numbers (on page 93).

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
Hitachi Remote Ops	HTTPS, FTP (SSL)	4431	Yes, only if Remote Ops 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 98).
- 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 94).

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 98))
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 93).

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.
- When changing a range of port numbers, enter a port range value that is greater than or equal to the number of ports associated with the number of storage systems registered in the Storage Device List.
- The available character strings in the effective range are as follows:

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

  To specify sequential values for the port number range, separate the values with a hyphen. For example, to specify the range between 5989 and 5991 for SMIS_CIMOM port numbers, type: `MappPortRangeSet.bat SMIS_CIMOM 5989-5991`.

  To specify nonsequential values for the port range, separate each value with a comma. For example, to specify the values 5989 and 5991 for SMIS_CIMOM port numbers, type: `MappPortRangeSet.bat SMIS_CIMOM 5989,5991`.

  You can also use a comma to specify one port number.For example, to specify 5989 for SMIS_CIMOM port number, type: MappPortRangeSet.bat SMIS_CIMOM 5989,5989

  If "rm" is specified, delete the setting of the specified port number key.

To remove the setting by each port number key name, use “rm” (for example, `PreRMIServer rm`).

- You can specify more than one command input parameter “[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.

Next steps

See Reallocating automatically allocated port numbers (on page 93) .

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.

Next steps

See Reallocating automatically allocated port numbers (on page 93) .

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.

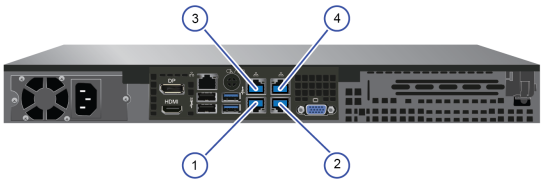
   Tip: `C:\MAPP` indicates the installation directory of the storage management software and SVP software. If the installation directory is not `C:\Mapp`, replace `C:\Mapp` with the appropriate installation directory.
3. The information of the port numbers to be used in the SVP is displayed. For the ports 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

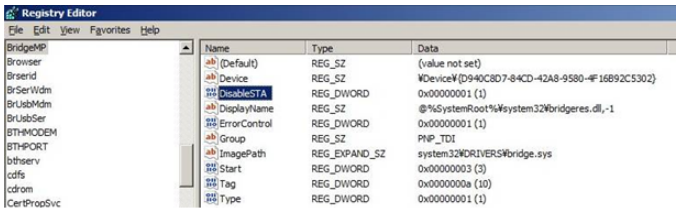
1. If your network uses the spanning tree protocol (STP) Bridge Protocol Data Unit (BPDU) guard on your network, perform the following Registry changes. Otherwise, skip to step 2:
   a. If you use the physical SVP supplied by Hitachi Vantara, verify the following connections.



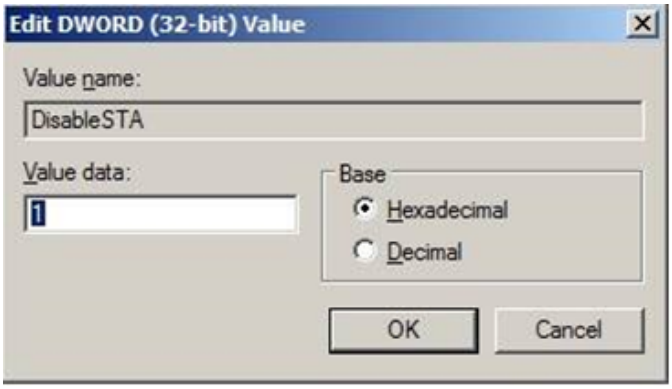
SVP LAN Port	Description
1	Do not connect a cable to the LAN 1 port at this time. You will connect to this port after you complete the **Initial Startup** wizard.
2	Connect the LAN 2 port to a Windows-based management console.
3	The LAN 3 port is already connected to the user LAN port on controller 1.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

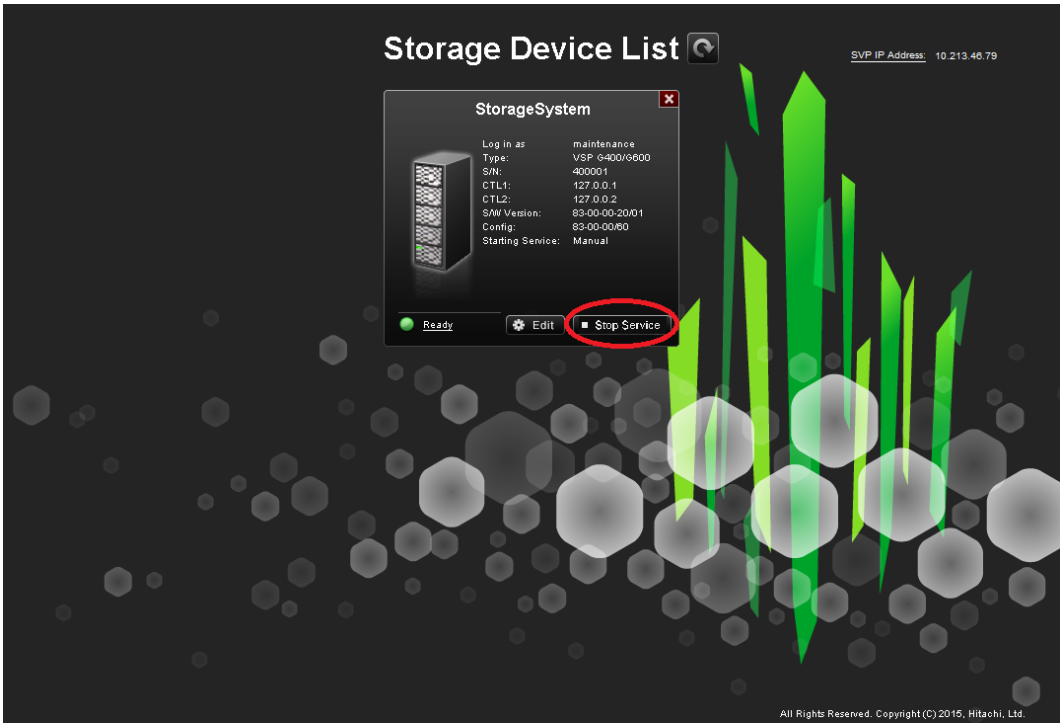


g. For the `DisableSTA` DWORD, change the hexadecimal **Value data** value to `1`, and then click **OK**.

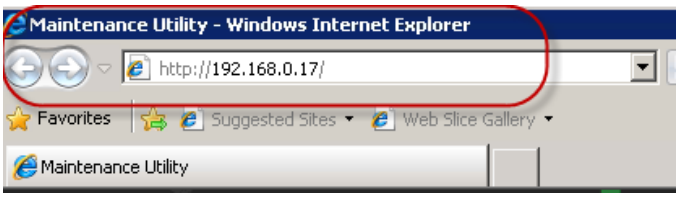


h. Restart the SVP, reconnect the cable to the **LAN1** port on the SVP, and verify connectivity through the network to the SVP.

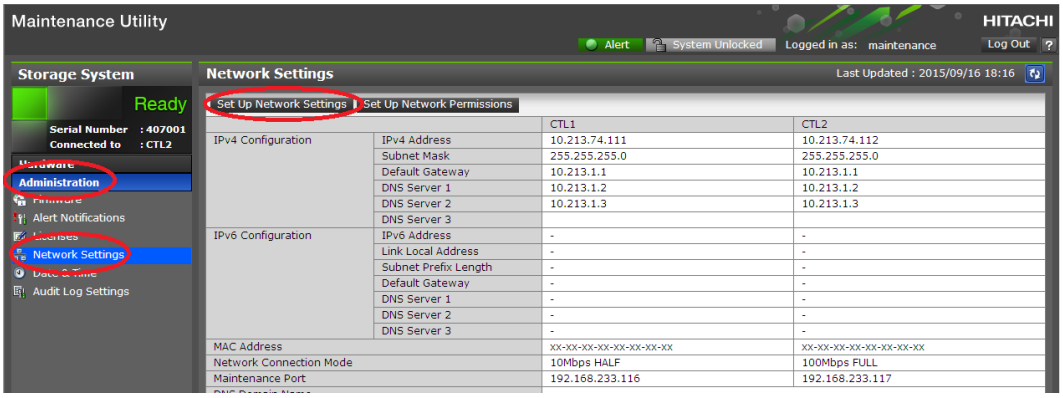
2. Using Remote Desktop Connection, access the SVP using the storage system's maintenance LAN port of `10.0.0.100`.
3. In the **Storage Device List** window, click **Stop Service**. Wait up to five minutes for the service to stop.



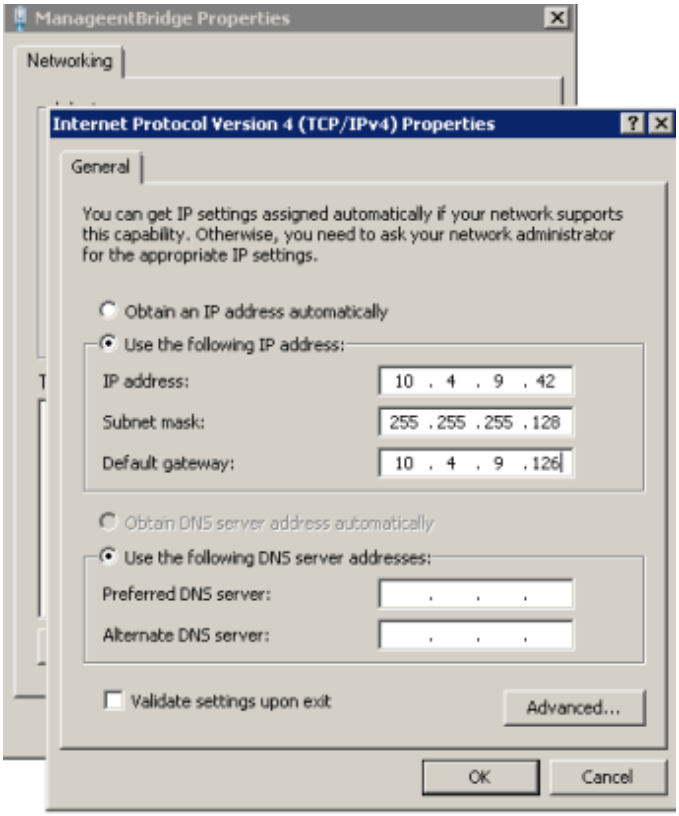
4. Log on to the maintenance utility.



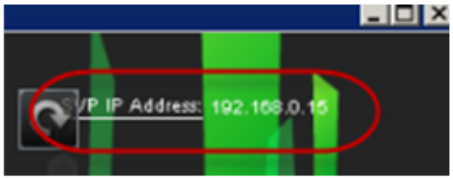
5. In the maintenance utility, click **Administration** > **Network Setting**, and then click **Set Up Network Settings**.



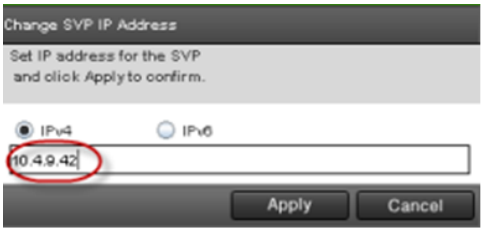
6. Change the CTL1 and CTL2 LAN IP addresses, as required.
7. Change the properties of the network bridge to reflect your IP address, subnet, and default gateway settings.



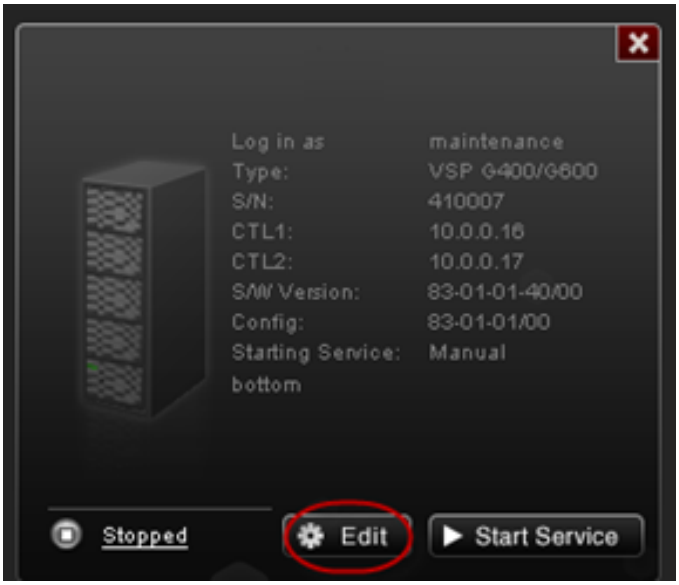
8. To verify that the new LAN IP settings are appropriate for your environment, exit to a command prompt (DOS) window and ping controller 1 and controller 2 using the new IP addresses. Do not proceed until this step is successful.
9. In the **Storage Device List** window, click the SVP IP address setting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



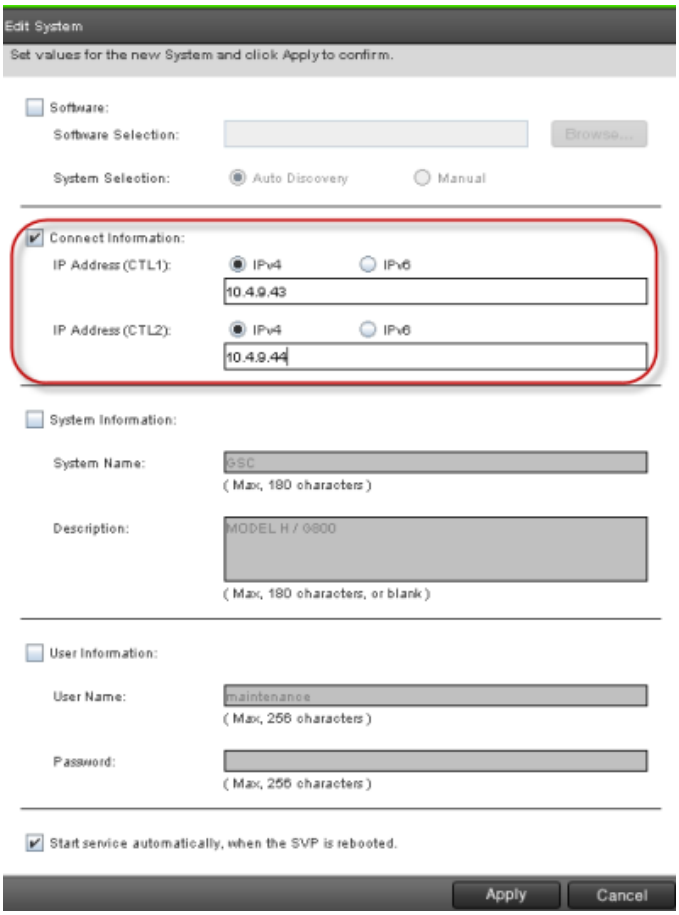
10. Change the SVP IP address to match the new bridge IP address setting, and then click **Apply**.



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



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



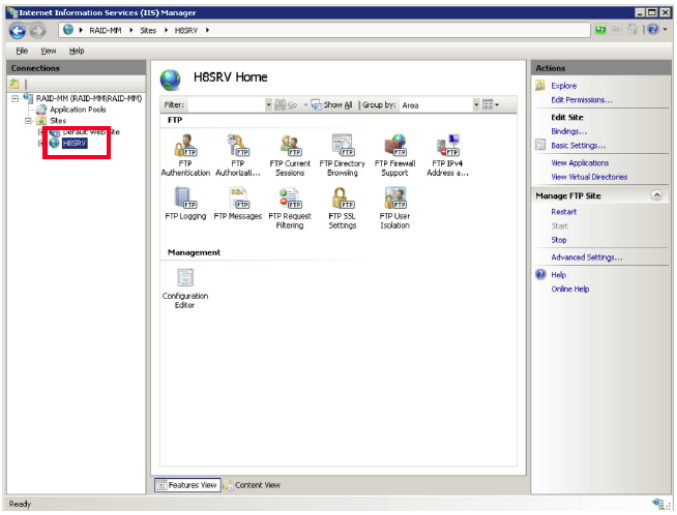
13. In the **Storage Device List** window, click **Start Service**. At the confirmation message, click **Confirm**.

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.

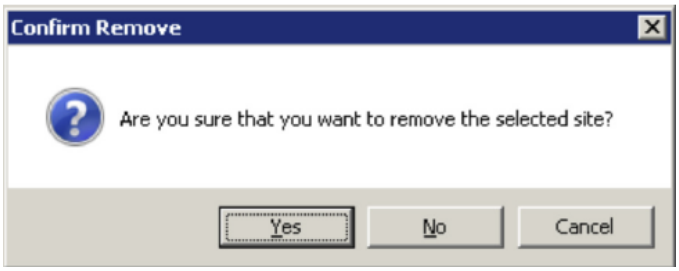
16. Verify information internet service (IIS) FTP settings.

a. Using a maintenance PC, from the Control Panel, open **Administrative Tools** and start **Internet Information Services (IIS) Manager**.

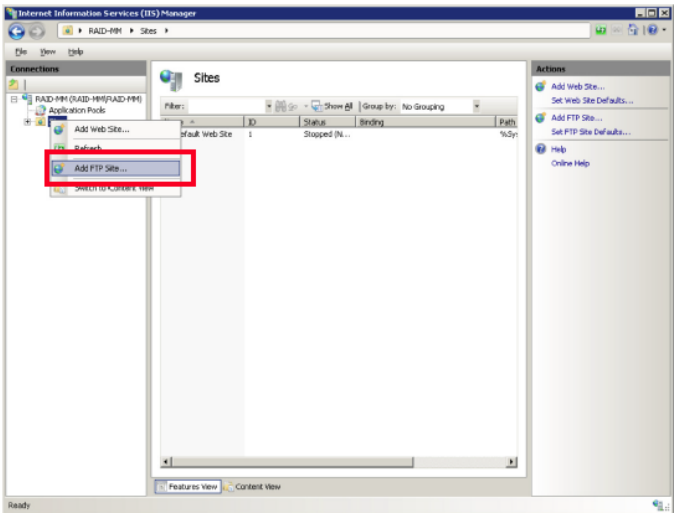
b. If the default website and the existing FTP server (including H8SRV) are registered, right-click the FTP server under **Sites**, and then click **Delete**.



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



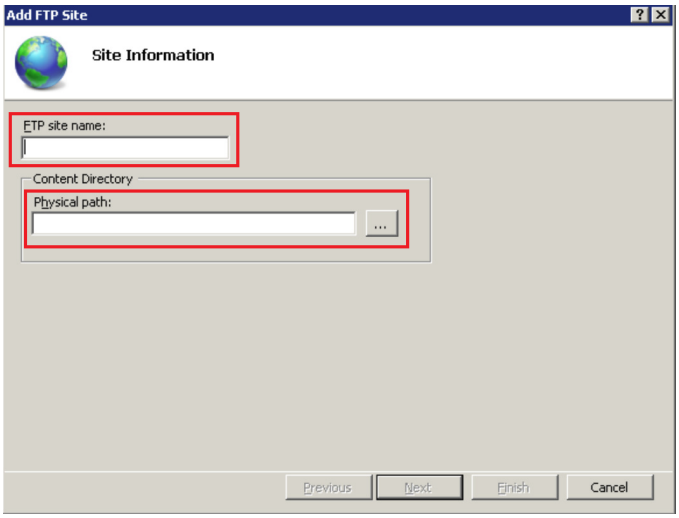
c. Right-click **Sites**, and then click **Add FTP Site**.



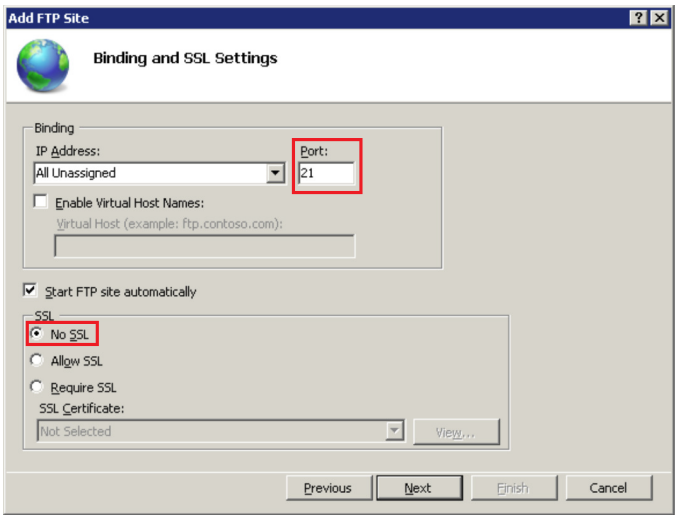
d. For **FTP site name**, type `H8SRV`. For **Content Directory**, type `C:\Mapp\wk\83xxxxyyyyyy\DKC200\HOME\micro`. Click **Next**.

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

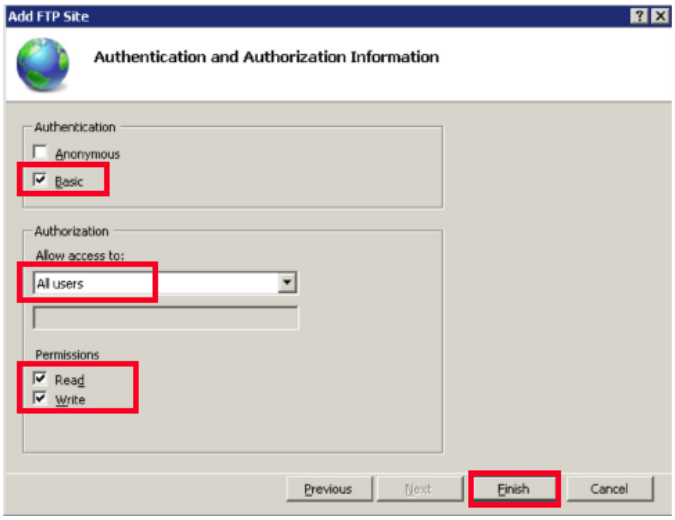
   - `6000`: VSP G800 or VSP F800
   - `4000`: VSP G400, G600 or VSP F400, F600
   - `2000`: VSP G200
   - `yyyyyy` = serial number



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

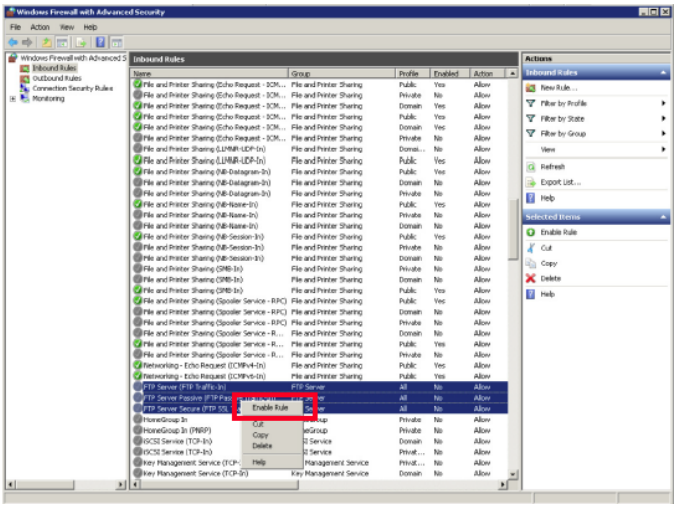


f. For **Authentication**, select **Basic**. For **Authorization**, select **All users**. For **Permissions**, select **Read** and **Write**. Click **Finish**.

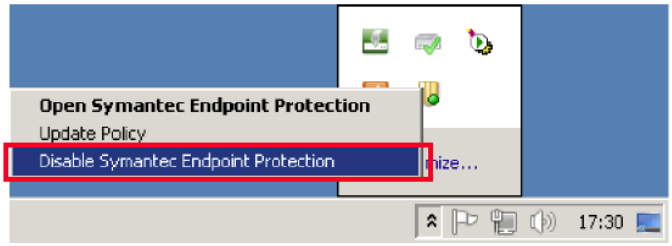


g. From the Control Panel, open **Administrative Tools** and start **Windows Firewall with Advanced Security**.

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**.



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**.



Chapter 16: Deleting and registering the storage system

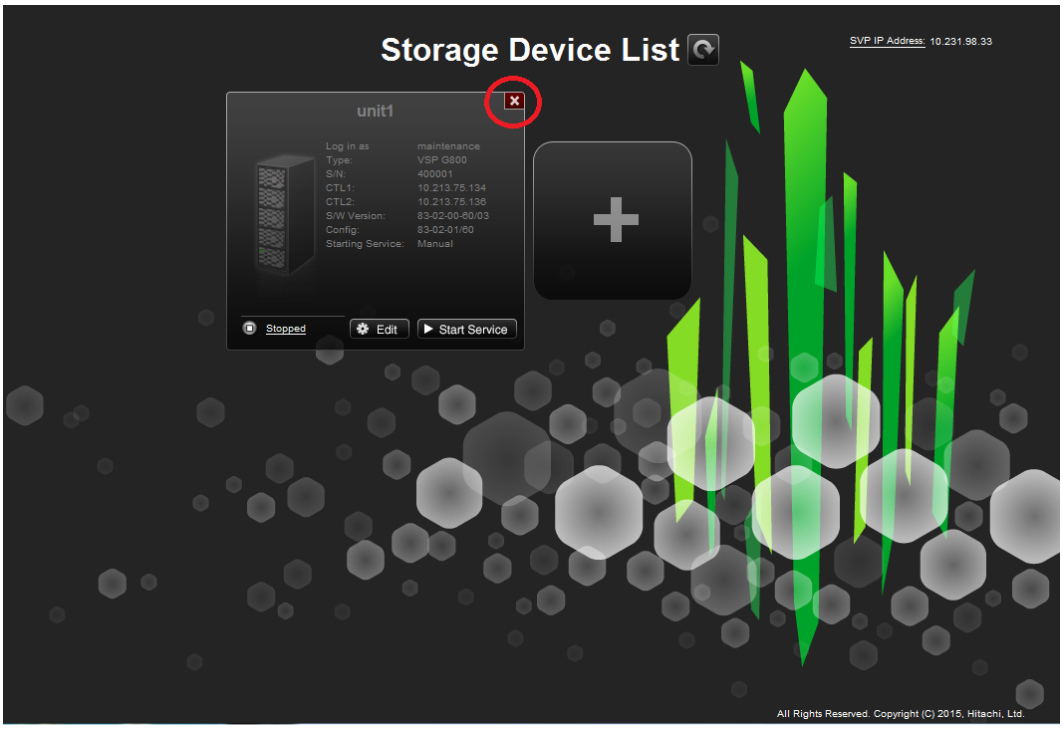
In the unlikely event you need to delete the storage system from the Storage Device List, use the following instructions to delete the storage system, and then register it on the SVP.

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).
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.



Registering the storage system on the SVP

The Storage Device List and Hitachi Device Manager - Storage Navigator are installed on the SVP. Only one Storage Device List is installed on the SVP, while the Device Manager - Storage Navigator is installed for each storage system registered in the Storage Device List. If you deleted the registered storage system from the SVP, you can register the storage system. For convenience, you can upgrade the storage system firmware as part of the registration process.

Before you begin

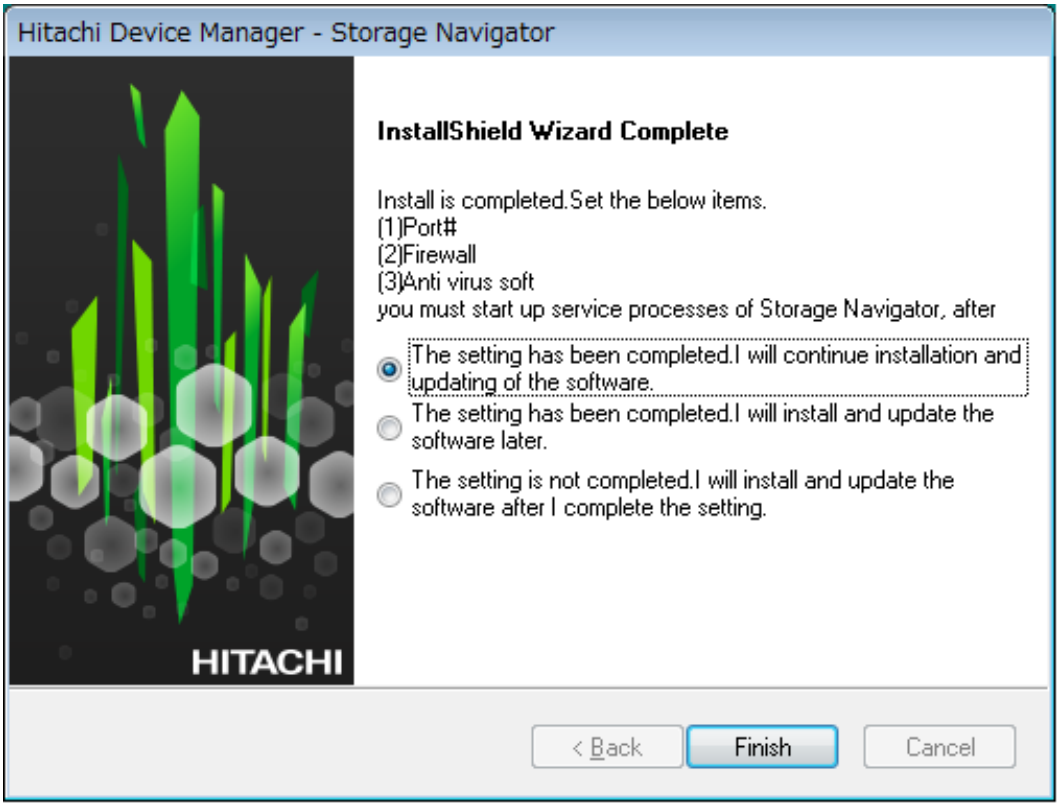
- Verify that the storage system to be registered is operating, and that the IP addresses of the SVP and the storage system are using the same subnet.
- Make sure the SVP hardware complies with the information under *SVP overview*.
- Make sure the supported OS version complies with the information under *SVP overview*.
- Make sure the management client is running Internet Explorer or Google Chrome.
- Make sure the supported TLS version is 1.2.
- Confirm that the VSP G200, G400, G600, G800 storage system is running software version 83-03-21-x0/xx or later.

Registering a storage system takes approximately 10 minutes. If you upgrade the firmware as well, the procedure can take approximately 200 minutes for each storage system.

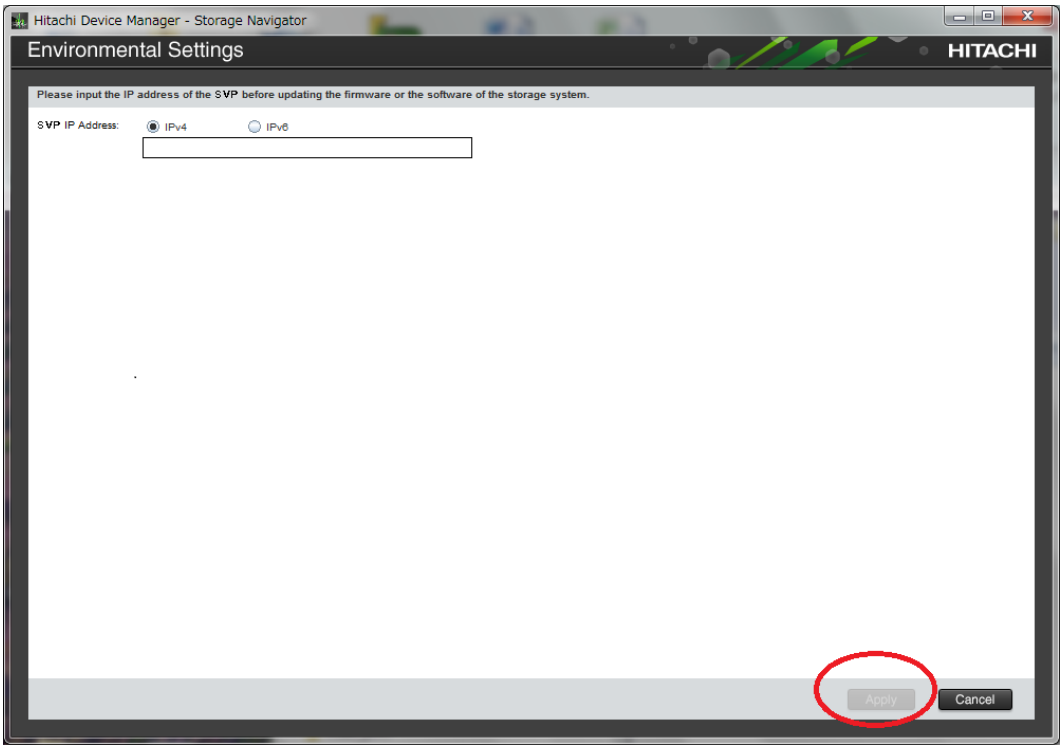
Note: The upgrade time can take up to 9 hours to complete when NAS modules are installed.

Procedure

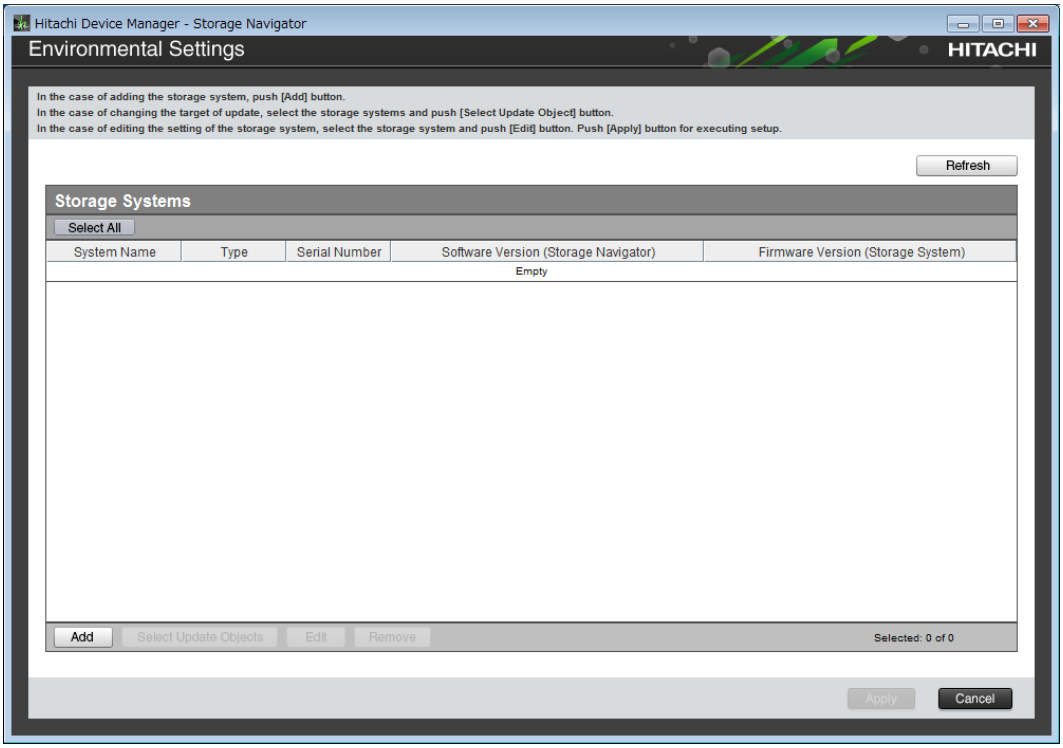
1. At the console PC connected to the physical SVP or running the SVP software, insert the media containing the SVP firmware media.
2. On the SVP, create a new folder, and then copy all of the files from the SVP firmware media into the new folder.
3. In the new folder, right-click the `Setup.exe` file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



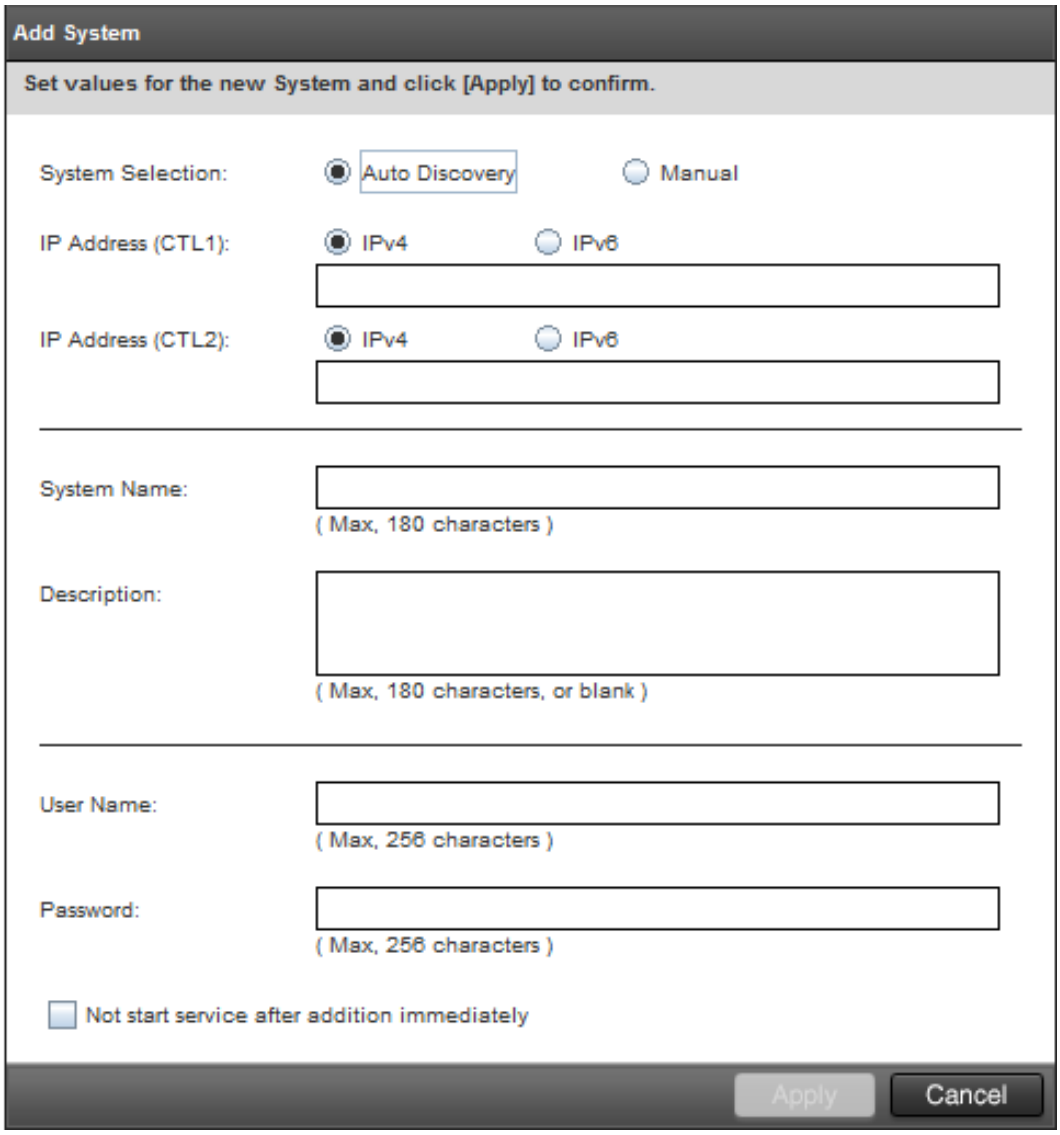
6. When prompted, select the IP addressing method (**IPv4** or **IPv6**), enter the IP address of the port connecting the SVP and the storage system, and then click **Apply**.



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



The **Add System** window opens.



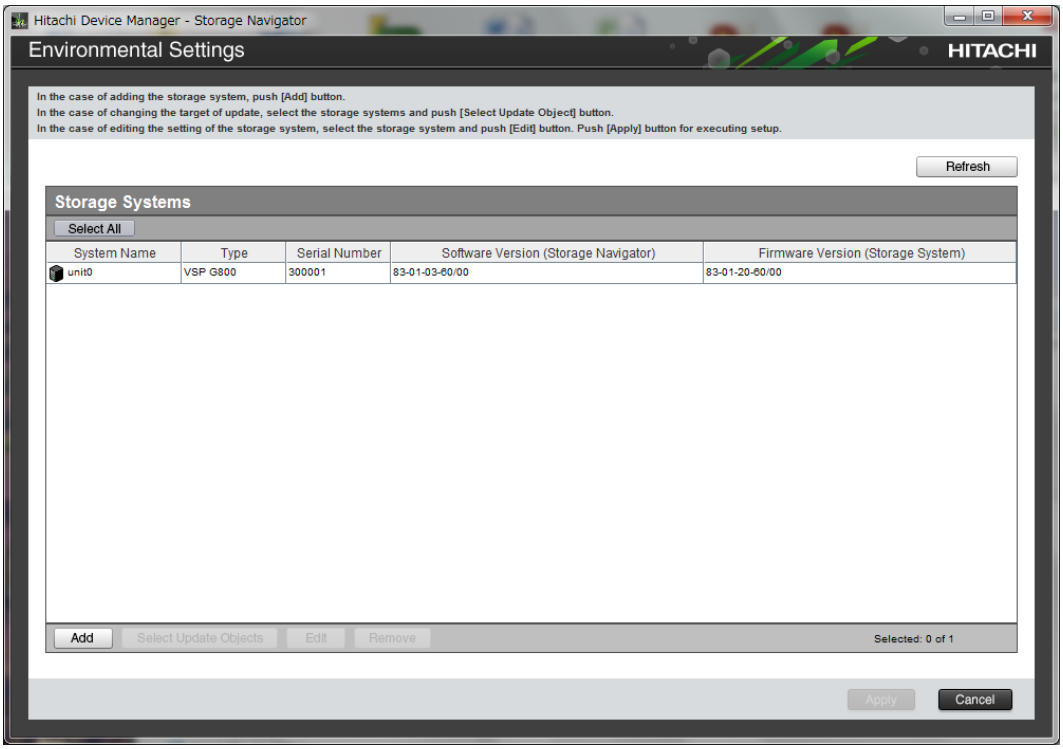
8. In the **Add System** window, complete the fields.

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.

Field	Description
IP Address (CTL 1)	Enter the IP address for controller 1. Accept the default **IPv4** setting or click **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 click the IP address in the appropriate format for the addressing method selected.
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 180 characters.
User Name	Enter a user name. Permitted characters are one-byte alphanumeric characters and symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~). The GUI includes a 256-character limit.
Password	Enter a password. The GUI includes a 256-character limit.
Do not start service after addition immediately[2]	Select if you do not want to start service after adding the storage system. (Default is unchecked.)
Notes: 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.	

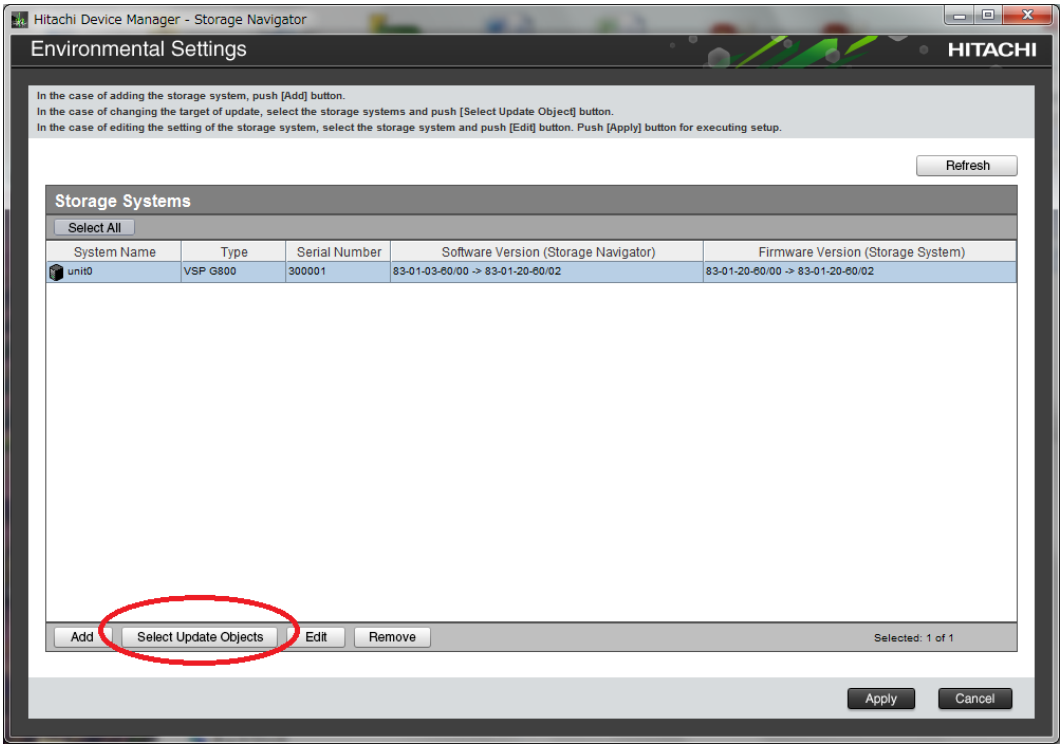
9. Click **Apply**.

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

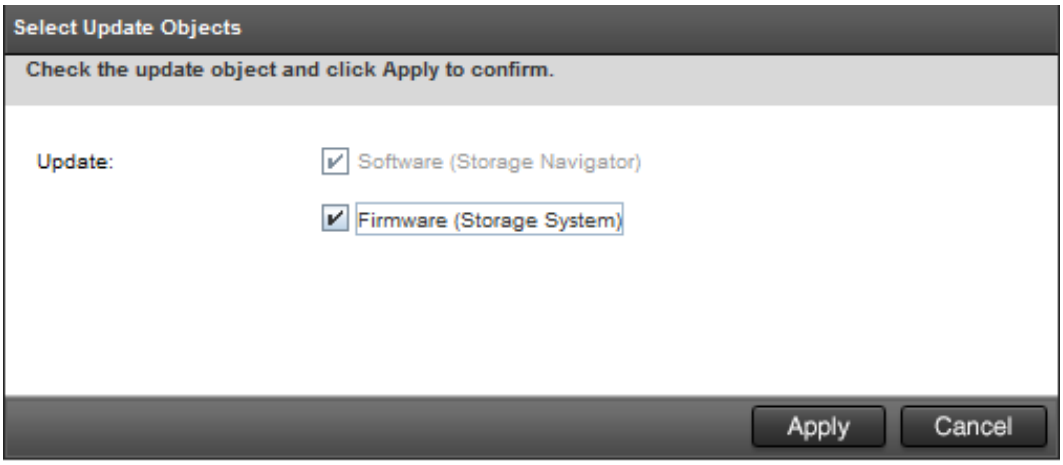


Note: If you added the wrong storage system, select it in the window, and then click **Remove**.

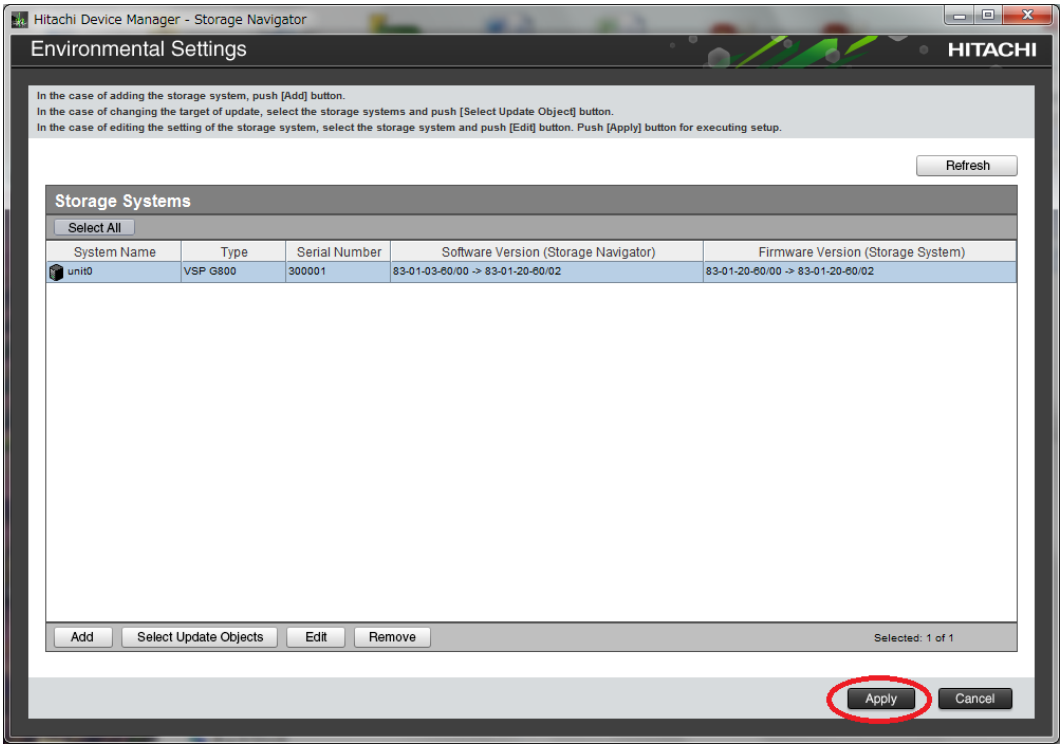
10. To update the firmware and add storage systems at the same time, select the storage systems and click **Select Update Objects**.



The **Select Update Objects** window opens.



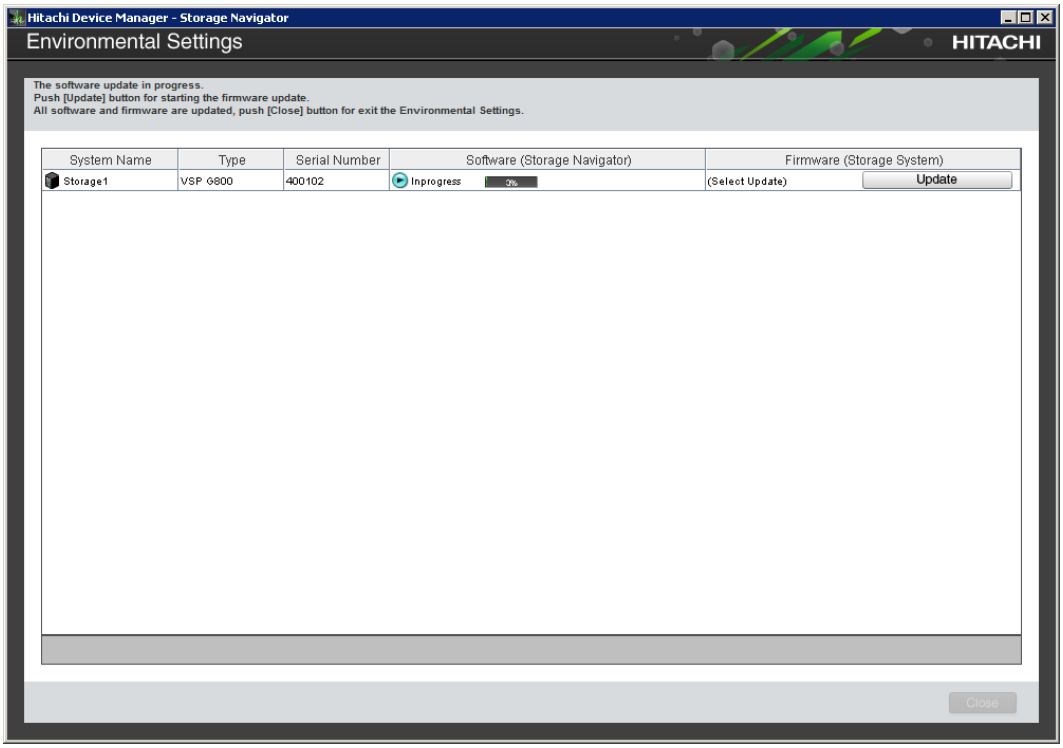
11. To update the firmware of the storage system being registered, check **Firmware (Storage System)**. Otherwise, leave it unchecked.
12. To register additional storage systems, repeat steps 6 through 10.
13. Click **Apply** in the **target storage system** list window.



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

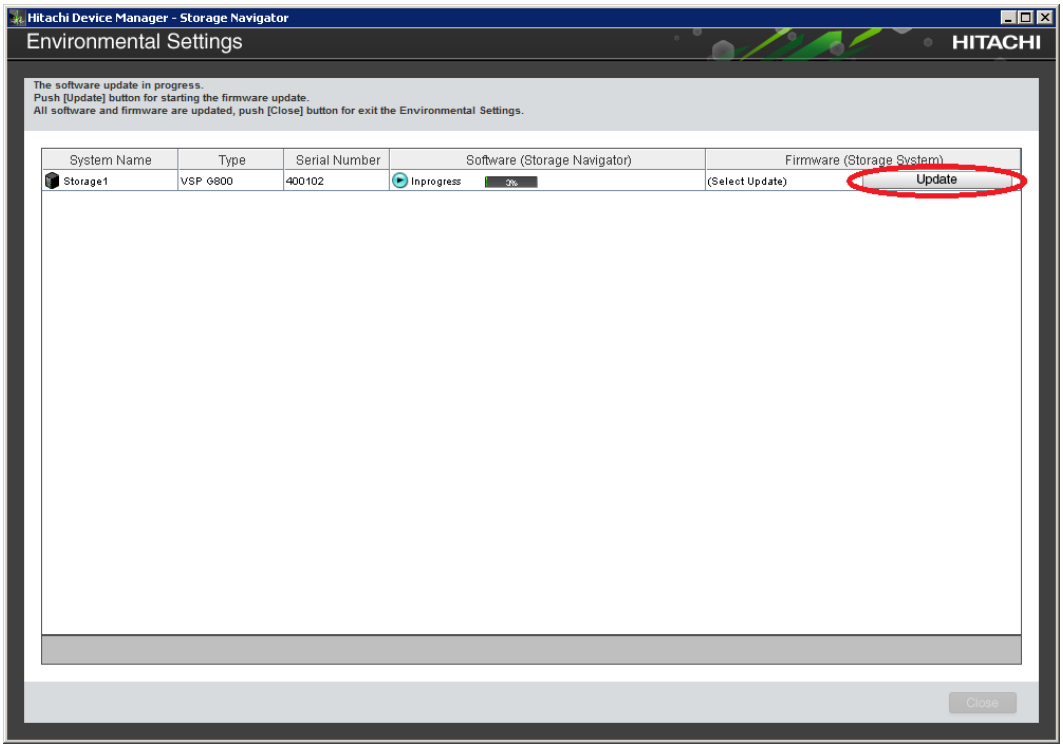
    The **Run Update Firmware** window opens and the upgrade starts automatically.

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.



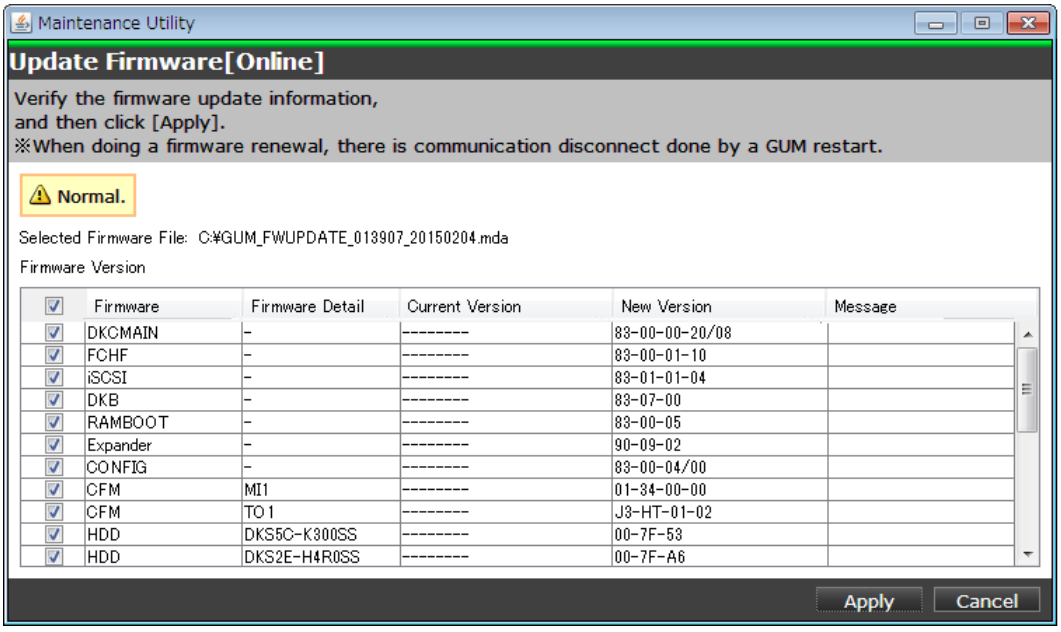
Status	Description
Waiting	One of the following: ▪ Software is not upgrading. ▪ Software components are being upgraded individually. If the software is already upgraded, this status refers to another storage system.
In progress	Software upgrade is running.
Completed	Software upgrade has completed.
Failed	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.

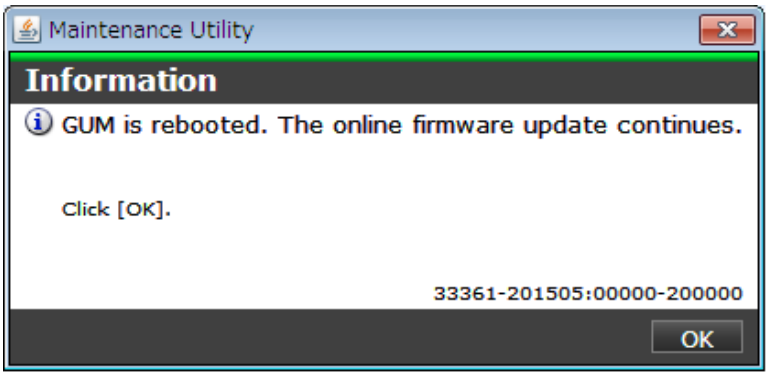


Note: If a window reports a problem with this website's security certificate, click **Continue to this website**, and then close the browser. If a **Java Update Needed** window opens, click **Later**. If a JRE **Security Warning** window opens, select the check boxes in each window and click **Continue**,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

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



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



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
Hitachi Remote Ops	No report from the agent during a 24-hour health check	Remote Ops detects SVP failure -> SVP replacement. Contact a Hitachi Vantara representative or authorized service provider.
Hitachi Command Suite	RMI connection error (not alert)	See the *Hitachi Command Suite Administrator Guide* (MK-90HC175).
Hitachi Ops Center Administrator	Hardware alerts appear in Alert tiles, along with drill-down views for detailed information.	See *Hitachi Storage Advisor User Guide* (MK-94HSA004).

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 E990	EDW-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
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact