



Hitachi Virtual Storage Platform G200, G400, G600

Service Processor Technical Reference

© 2015 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi, Ltd.

Hitachi, Ltd., reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. This document contains the most current information available at the time of publication. When new or revised information becomes available, this entire document will be updated and distributed to all registered users.

Some of the features described in this document might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at <https://portal.hds.com>.

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

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

- a) Acquiring the relevant consents as may be required under local privacy laws or otherwise from employees and other individuals to access relevant data; and
- b) Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

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

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

AIX, AS/400, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, RS/6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, z10, zSeries, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

iPad is a trademark of Apple Inc., registered in the U.S. and other countries.

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

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

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

Equipment warranty

The term of guarantee of normal operation of the storage system and free service is one year from date of purchase.

If a failure occurs multiple times, the storage system might shut off to avoid a serious accident.

Notice of export controls

Export of technical data contained in this document might require an export license from the United States government, the government of Japan. or both. Contact the Hitachi Legal Department for guidance about any export compliance questions.

Backup

Hitachi cannot guarantee against data loss due to failures. Therefore, back up your data to minimize chances for data loss.

Data backup is also critical when hardware components are added or replaced, because performing such hardware procedures restores parameter settings that can affect how data is managed on the storage systems.

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 law, must be recycled.

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



UEFI Development Kit 2010

This product includes UEFI Development Kit 2010 written by the UEFI Open Source Community. For more information, see the UEFI Development Kit website:

<http://sourceforge.net/apps/mediawiki/tianocore/index.php?title=UDK2010>

© 2004, Intel Corporation.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Intel Corporation nor the names of its contributors might be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Notes on use

When using the Hitachi storage system, be sure to read this guide and understand the operating procedures and instructions described herein thoroughly before starting your operation.

The array complies with FDA radiation performance standard 21 CFR subchapter J.

EMI regulation

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference in which case the user will be required to correct the interference at his own expense. Testing was done with shielded cables. Therefore, in order to comply with the FCC regulations, you must use shielded cables with your installation.

The electromagnetic interference (EMI) test was done in the following configuration.

If trouble occurs in another configuration, a user might be requested to take appropriate preventative measures:

- RKU CBSS dense intermix drive tray flash module drive tray+2 small form factor drive trays + 1 large form factor drive tray.
- RKU CBSL 1 small form factor drive tray
- RKU CBL dense intermix drive tray flash module drive tray 3 small form factor drive trays 3 large form factor drive trays

This product must not be used in residential areas.

This is a class A product. In a domestic environment this product can cause radio interference in which case the user can be required to take adequate measures.



Contents

Preface - SVP.....	11
Intended audience.....	12
Document conventions.....	12
Conventions for storage capacity values.....	13
Accessing product documentation.....	13
Getting help.....	14
Comments.....	14
1 Overview.....	15
SVP hardware description.....	16
SVP front panel.....	16
SVP rear panel.....	17
SVP hardware specifications.....	17
SVP electrical specifications.....	18
SVP network configuration.....	19
Physical LAN port assignment.....	19
Default IP address settings.....	20
2 Installing the SVP.....	23
Mounting the SVP.....	24
Mounting the SVP.....	25
Choose a mounting location.....	25
Installing the inner rail extension.....	25
Installing the outer rails to the rack.....	27
Installing the chassis into the rack.....	27
Connecting to the SVP.....	28
Powering up the SVP.....	29
Setting the SVP date, time, and timezone settings.....	31
Disconnecting from the SVP.....	34

3 SVP support.....	37
Security patch and antivirus software policy.....	38
Online update.....	39
Offline update.....	39
Maintenance process.....	40
SVP failure detection.....	40
FRU replacement.....	41
Operating system recovery.....	41
Backing up the OS.....	42
Restoring the OS.....	42
Creating a network bridge.....	42
Powering off the SVP.....	43
Rebooting the SVP.....	44
Backing up the SVP configuration.....	44
Restoring the SVP configuration.....	45
Changing the SVP IP address.....	46
Changing the SVP IP address in Windows 7.....	46
Changing the SVP IP address using the Storage Device List.....	46
Deleting the registered storage system.....	47
Registering the storage system on the SVP.....	48
Blocking communications to port 80.....	53
 Index.....	 0



Preface - SVP

- [Intended audience](#)
- [Document conventions](#)
- [Conventions for storage capacity values](#)
- [Accessing product documentation](#)
- [Getting help](#)
- [Comments](#)

Intended audience

This document is intended for system administrators, Hitachi Data Systems representatives, and authorized service providers who install, configure, or operate Hitachi Virtual Storage Platform G200, G400, G600 storage systems.

Readers of this document should be familiar with the following:


- Data processing and RAID storage systems and their basic functions.
- The Hitachi Virtual Storage Platform G200, G400, G600 storage system.
- The operating system and web browser software on the system hosting the storage management software.




Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click OK .
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: <i>copy source-file target-file</i> Note: Angled brackets (< >) are also used to indicate variables.
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairdisplay -g oradb</code>
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: <code>pairdisplay -g <group></code> Note: Italic font is also used to indicate variables.
[] 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.

Icon	Label	Description
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions or consequences (for example, disruptive operations).
	WARNING	Warns the user of severe conditions or consequences (for example, destructive operations).

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

Logical capacity unit	Value
1 block	512 bytes
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 the Hitachi Data Systems Portal: <https://portal.hds.com>. 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 Data Systems Support Portal](#) is the destination for technical support of your current or previously-sold storage systems, midrange and enterprise servers, and combined solution offerings. The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the Hitachi Data Systems Support Portal for contact information: <https://portal.hds.com>.

[Hitachi Data Systems Community](#) is a new global online community for HDS customers, partners, independent software vendors, employees, and prospects. It is an open discussion among these groups about the HDS portfolio of products and services. It is the destination to get answers, discover insights, and make connections. The HDS Community complements our existing Support Portal and support services by providing an area where you can get answers to non-critical issues and questions. **Join the conversation today!** Go to community.hds.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hds.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 Data Systems Corporation.

Thank you!



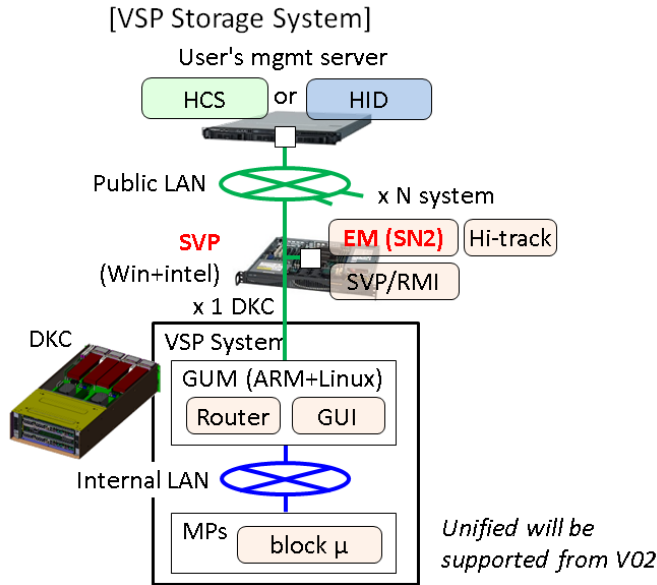
1

Overview

- [SVP hardware description](#)
- [SVP hardware specifications](#)
- [SVP electrical specifications](#)
- [SVP network configuration](#)

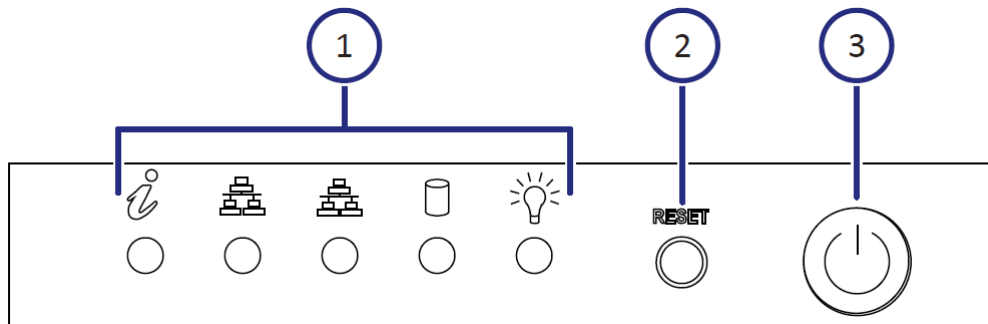
SVP hardware description

The SVP is a 1RU management server that attaches to each VSP disk controller (DKC).



SVP front panel

The SVP front panel has LEDs, a reset button, and a power button.

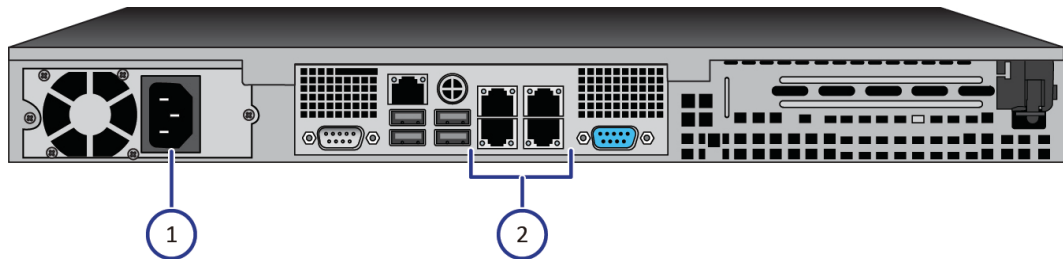


Number	Description
1	LEDs. From left to right, the LEDs are: <ul style="list-style-type: none"> BMC Heartbeat LAN card 2 LAN card 1

Number	Description
	<ul style="list-style-type: none"> Hard drive System standby power
2	Reset button.
3	Power button. Applies power to or removes power from the SVP.

SVP rear panel

The only ports used on the rear panel of the SVP are the power socket and the four LAN ports.



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

SVP hardware specifications

The following table lists the SVP hardware specifications.

Item	Specification
Dimensions	<p>Height: 1.7 inches (43 mm)</p> <p>Width: 17.2 inches (437 mm)</p> <p>Depth: 14.5 inches (369 mm)</p> <p>Weight: 14 lbs (6.4 kg)</p>
Processor	Celeron G1820 2.7 GHz 2M, 2C, 2T

Item	Specification
Memory	8 GB RAM DDR3
Hard drive	2 TB
Network interface card	x4 ports (on-board NIC) + x1 IPMI (BMC) port
Rated AC voltage	100-240 V, 50-60 Hz, 4.2 - 1.8A
Power supply	350 Watt AC power supply w/ PFC
AC voltage	100-240 V, 50-60 Hz, 4.2-1.8 Amp
Power supply safety / EMC	<ul style="list-style-type: none"> • USA - UL listed, FCC • Canada - CUL listed • Germany - TUV Certified • Europe/CE Mark • EN 60950/IEC 60950-Compliant
Fans	2x 4cm 4-pin PWM fans
Operating system	Microsoft Windows Embedded Standard 7
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)
Manufacturer	Super Micro (via Synnex)

SVP electrical specifications

The following table lists the SVP electrical specifications.

Mft. p-code	Description	Watts
MBD-X10SLM+-LN4F-O	Single-socket H3 (LGA 1150) / 32GB DDR3 ECC 1600MHz / 6x SATA / 4 x GbE	20
CSE-512F-350B	350W, 2x 3.5 Internal drive bays	26.4
CM8064601483405	Intel Celeron G1820 2.7 GHZ 2 M Tray	53
0F11000	3.5-inch 25.4 mm 2 TB 32 MB 7200 RPM	9.1
KVR16E11S8	4 GB 1600 MHZ DIMM SR X8 with TS Kingston F	4.05
		112.55 Watts Total

VA is 140.69, with a 0.8 power factor.

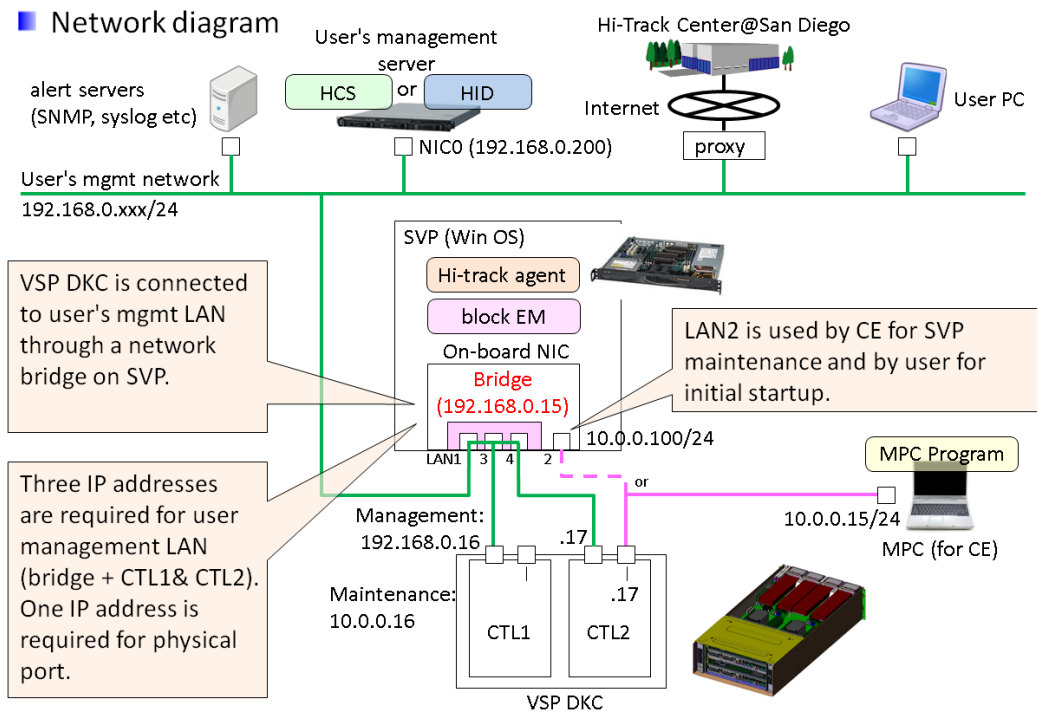


Note: These figures are not kilo values.

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 SVP, a network bridge refers to configuring the four onboard local-area network (LAN) ports using the Bridge Connections setting in the Microsoft Windows operating system. This arrangement obviates the need for an external switching hub.

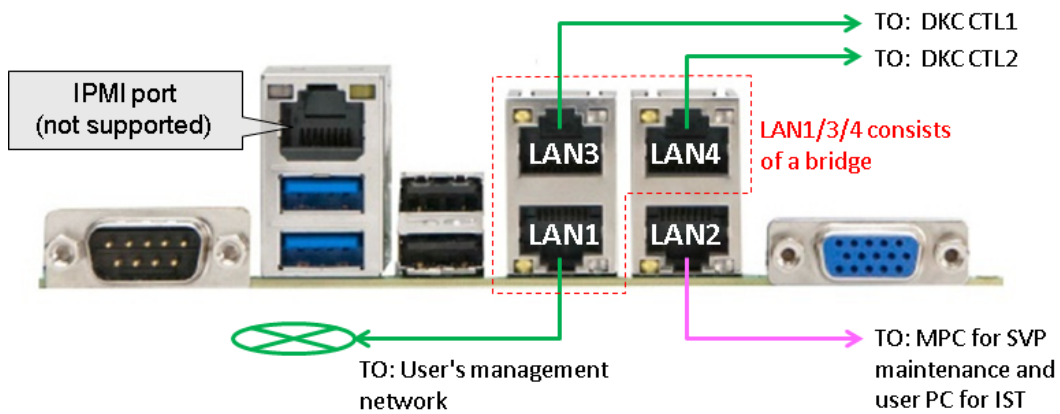
The following figure shows the SVP network configuration.



Physical LAN port assignment

The following figure shows the physical LAN port assignments on the SVP.

The IPMI port is an IPMI-dedicated port connected to the BMC in the SVP and is invisible from the Windows operating system. The IPMI port can be used if enabled in BIOS setting, but is not supported for the SVP.



Default IP address settings

The following table shows the SVP default IP addresses.

The bridge setting is configured at the Distribution Center. The user connects to the SVP using the IP address 192.168.0.15 for LAN1/3/4 ports (management) or 10.0.0.100 for LAN2 port (maintenance), respectively

Port	Name of NIC (user can change a NIC name)	Connected to	Default IP address	IP address after bridge is configured	Notes
LAN1	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).
LAN2	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.
LAN3	Management (CTL1)	DKC CTL1	n/a (DHCP)	192.168.0.15/24	Part of the bridge.
LAN4	Management (CTL2)	DKC CTL2	n/a (DHCP)	192.168.0.15/24	Part of the bridge.
IPMI	n/a	User PC	n/a (disabled) To enable IPMI LAN, change the BMC network configuration on the BIOS menu from	<--	Not supported (up to user).

			"Update IPMI LAN configuration" = "No" to "Yes" and perform the appropriate IP address setting.		
--	--	--	---	--	--

2

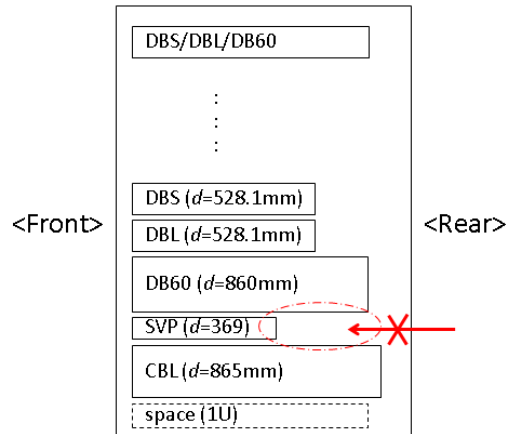
Installing the SVP

- [Mounting the SVP](#)
- [Mounting the SVP](#)
- [Connecting to the SVP](#)
- [Powering up the SVP](#)
- [Setting the SVP date, time, and timezone settings](#)
- [Disconnecting from the SVP](#)

Mounting the SVP

The SVP has a depth of 14.5 inches (369 mm), while 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 dense intermix drive tray, as shown below, there will not be enough space to access rear I/O panel of the SVP.

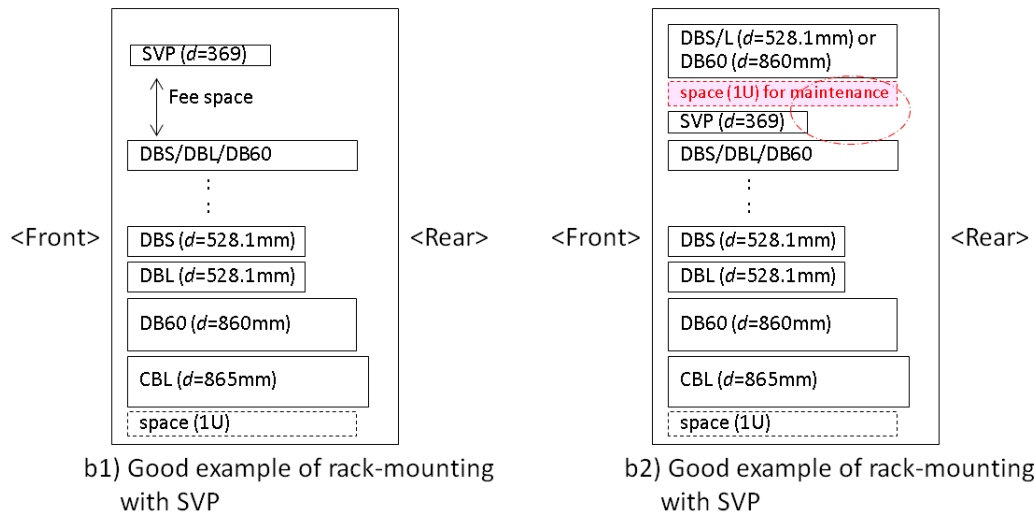


Rear I/O panel layout of SVP

a) Bad example of rack-mounting with SVP

To ensure that 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 dense intermix drive tray (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 dense intermix drive trays.



Mounting the SVP

The SVP comes with 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.

Use the following procedures to mount the SVP in a rack.

Choose a mounting location

Procedure

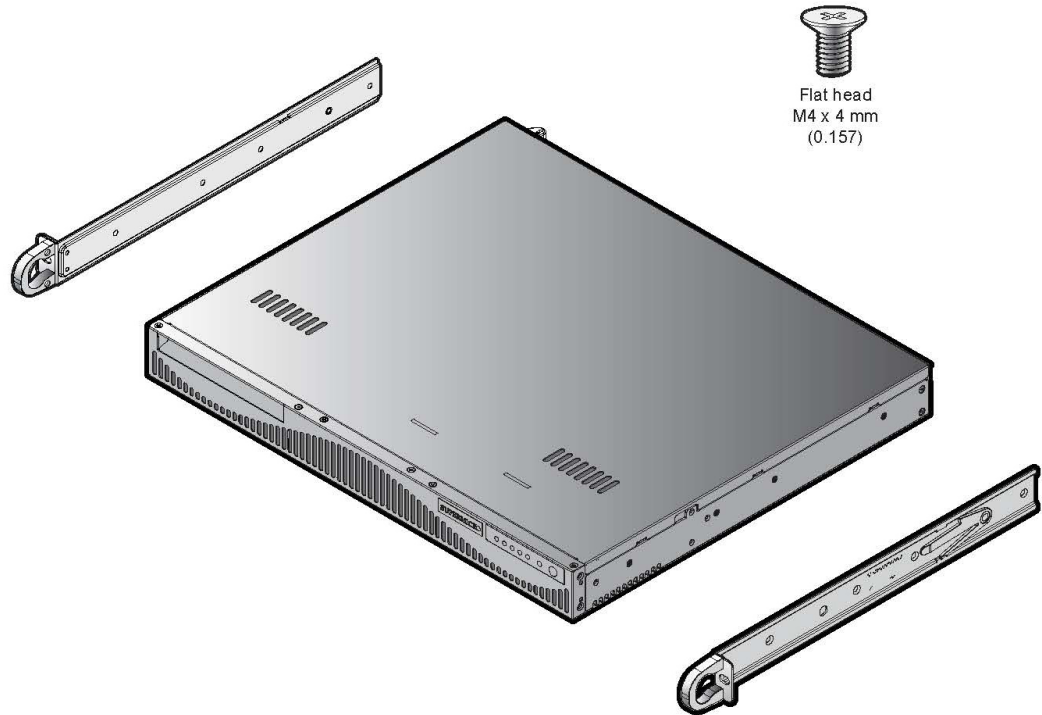
1. Install the SVP in the top bay of the rack.
2. Leave enough distance in front of the rack to enable you to open the front bezel (approximately 25 inches).
3. Leave approximately 30 inches of clearance in the back of the rack to allow for sufficient airflow and ease in servicing.

Installing the inner rail extension

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

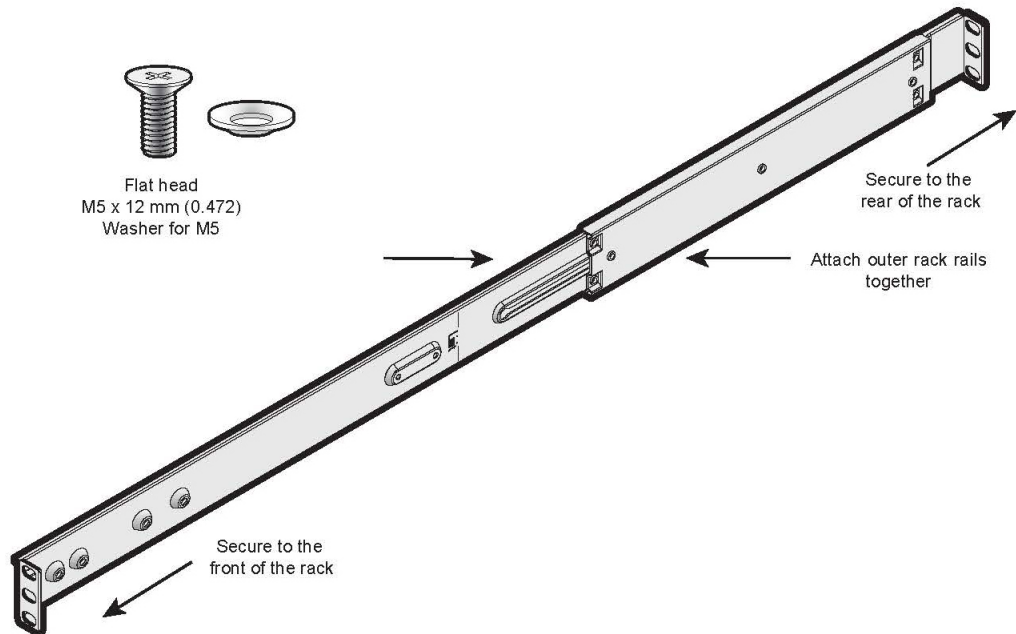
Procedure

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



2. Place the inner rail on the side of the chassis aligning the hooks of the chassis with the rail holes.
3. Slide the rail toward the front of the chassis to secure the rail in place.
4. Secure the chassis with four screws.

- Repeat steps 2 through 4 for the other inner rail extension.



Installing the outer rails to the rack

Procedure

- Attach the short bracket to the outside of the long bracket.
You must align the pins with the slides. Orient both bracket ends so they face the same direction.
- Adjust both the short and long brackets to the proper distance so the rail fits snugly into the rack.
- Secure the long bracket to the front side of the outer rail with two M5 screws and the short bracket to the rear side of the outer rail with three M5 screws.
Use a washer with each screw.
- Repeat steps 1 through 3 for the left outer rail.

Installing the chassis into the rack

Prerequisites

- The inner rails are attached to the chassis.
- The outer rails are installed on the rack.

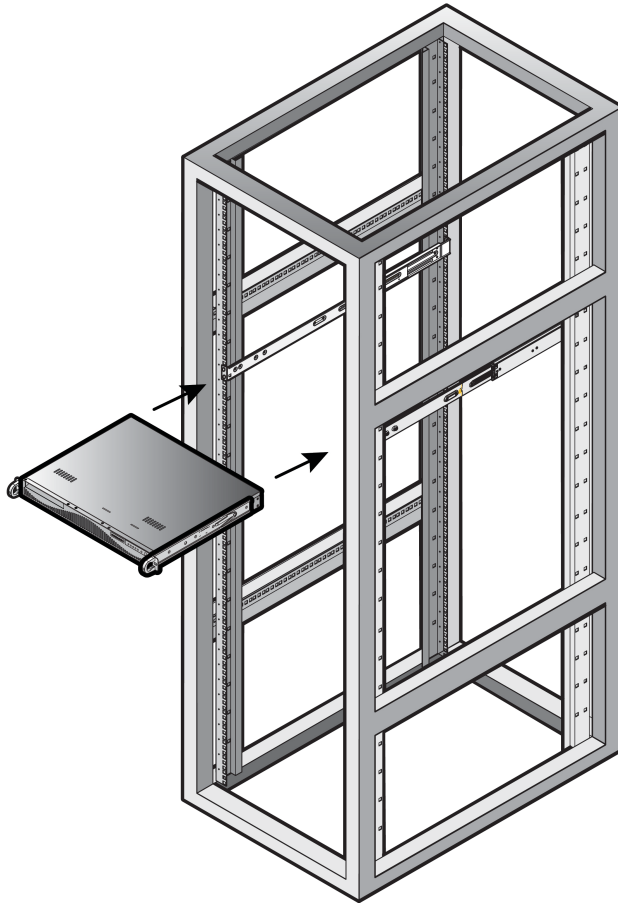
Procedure

1. Align chassis rails with the front of the rack rails.
2. Slide the chassis rails into the rack rails, keeping the pressure even on both sides.

If necessary, press the locking tabs when inserting.

When the server is pushed completely into the rack, the locking tabs "click" into the locked position.

3. Optional: Insert and tighten the thumbscrews that hold the front of the server to the rack.



Connecting to the SVP

The rear panel of the SVP has four RJ-45 ports. Using Category 5 or better Ethernet cables, perform the following connections on the SVP. Your management console must be able to access the SVP.

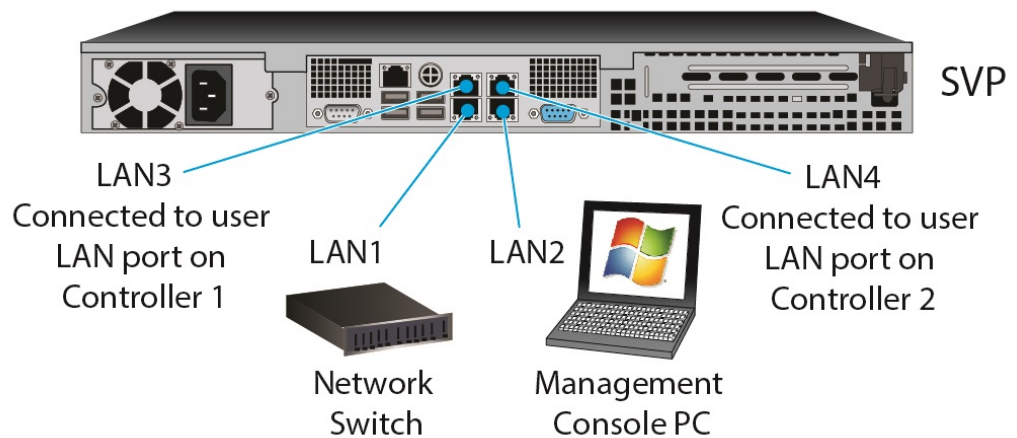
Procedure

1. Connect **LAN1** 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 **LAN2** to a management console PC.
Typically, this is a notebook PC.
3. Connect **LAN3** to the user LAN port on storage system controller 1.
4. Connect **LAN4** to the user LAN port on storage system controller 2.



Powering up the SVP

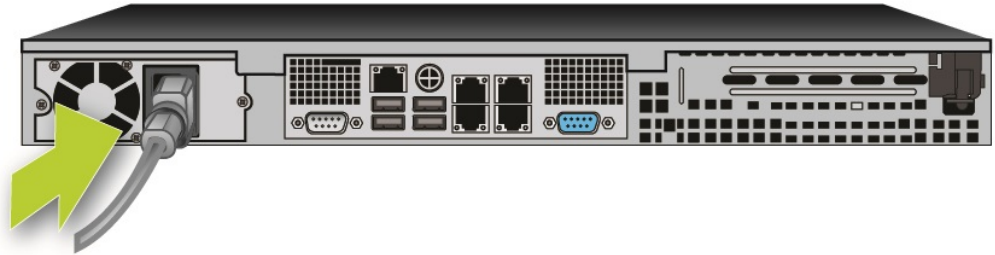
Prerequisites

Power up the SVP before you power up the storage system.

Procedure

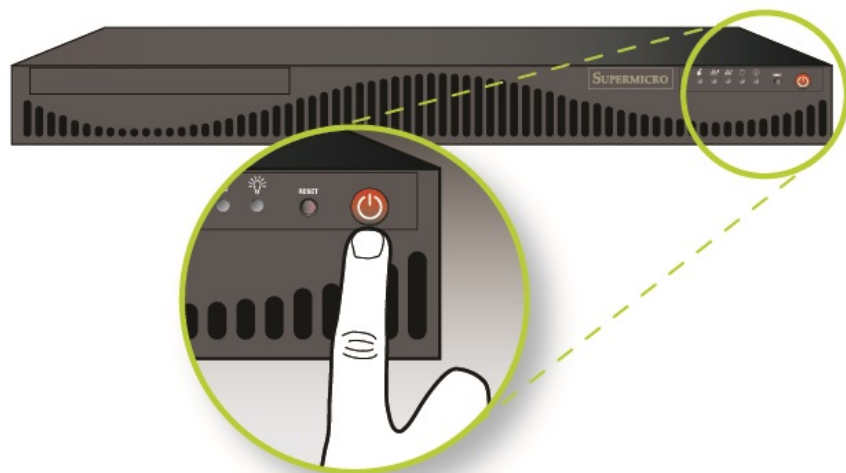
1. Attach the supplied power cable to the power socket on the rear panel of the SVP.

SVP (rear)



2. Plug the other end of the power cable into an AC power source.
3. Push the power button on the front of the SVP.

SVP
(front)



Setting the SVP date, time, and timezone settings

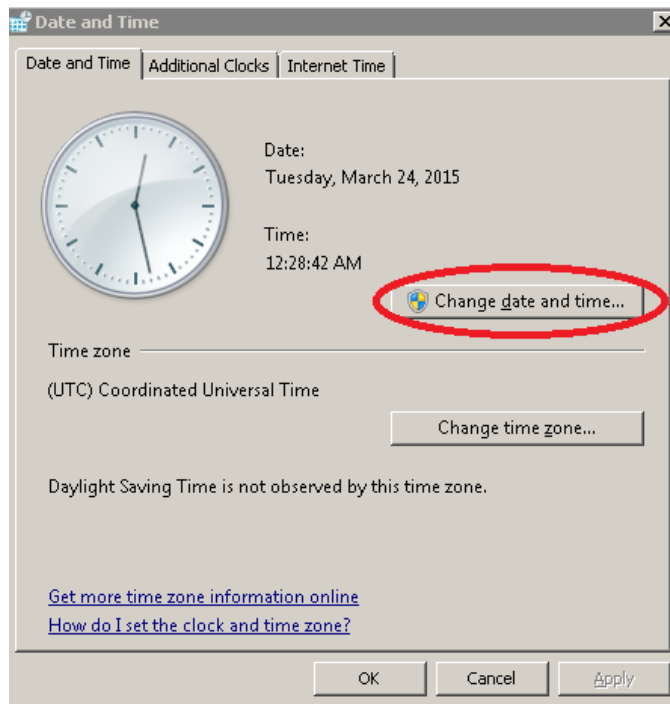
Set the SVP date, time, and timezone to the local time where the SVP is installed. You specify these settings using the Microsoft Windows 7 operating system running on the SVP.

You perform this procedure using the management console PC. This procedure assumes the following:

- The management PC is connected to the LAN 2 port on the SVP.
- The PC has established a Remote Desktop Connection with the SVP.
- The **Management Utility** window is displayed on the PC.

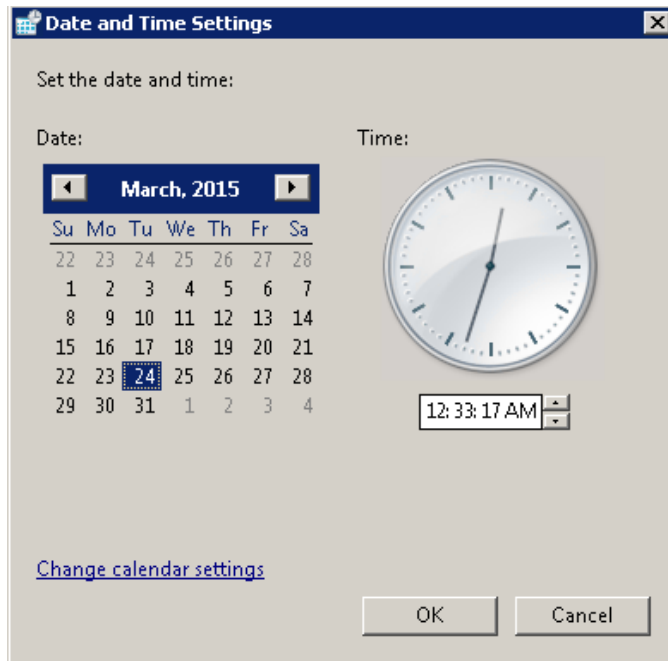
Procedure

1. In the desktop, click the **Start** button, and then click **Control Panel**.
2. Click **Clock, Language, and Region**.
The **Clock, Language, and Region** window appears.
3. Click **Date and Time**.
The **Date and Time** window appears, with the **Date and Time** tab displayed.



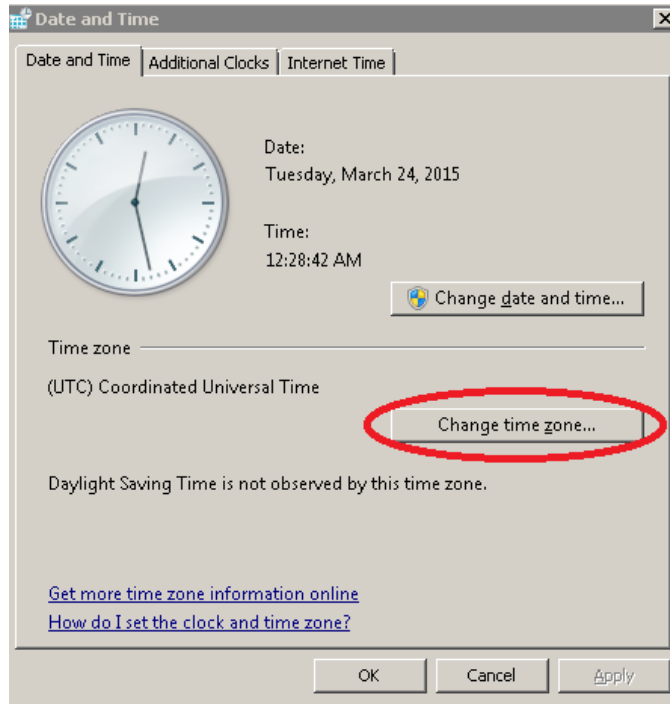
4. Click **Change date and time**.
The **Date and Time Settings** window appears.

5. Set the year, month, day, and time.



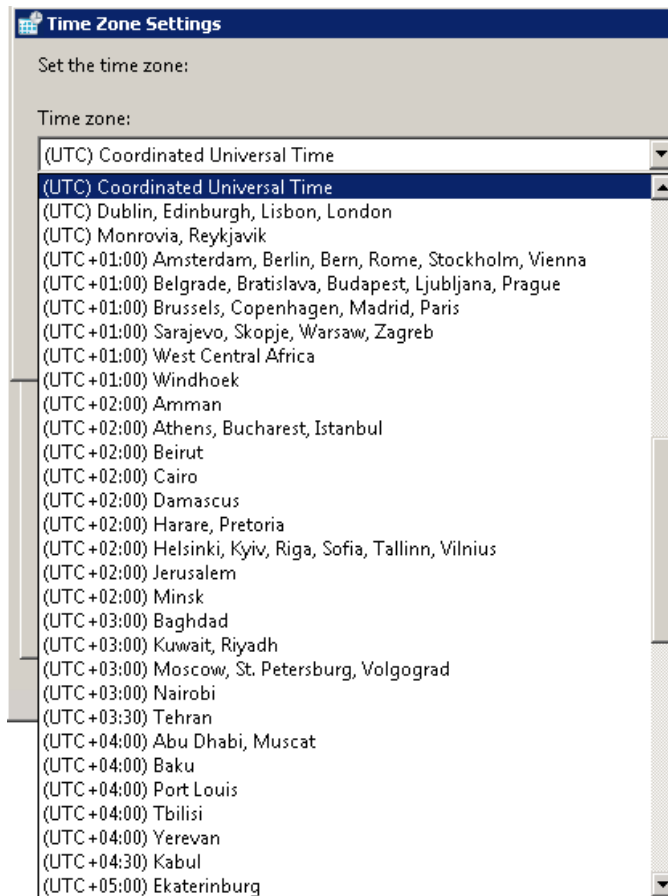
6. Click **OK**.

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



The Time Zone Settings window appears.

8. Select a UTC timezone from the drop-down list, and then click **OK**.



9. Click **OK**.
10. Close the Windows Control Panel.

Disconnecting from the SVP

To disconnect the management console PC from the SVP:

Procedure

1. Click the **Start** button on the SVP desktop.

2. Click **Log off > Disconnect**.



Result

The SVP disconnects from the PC.

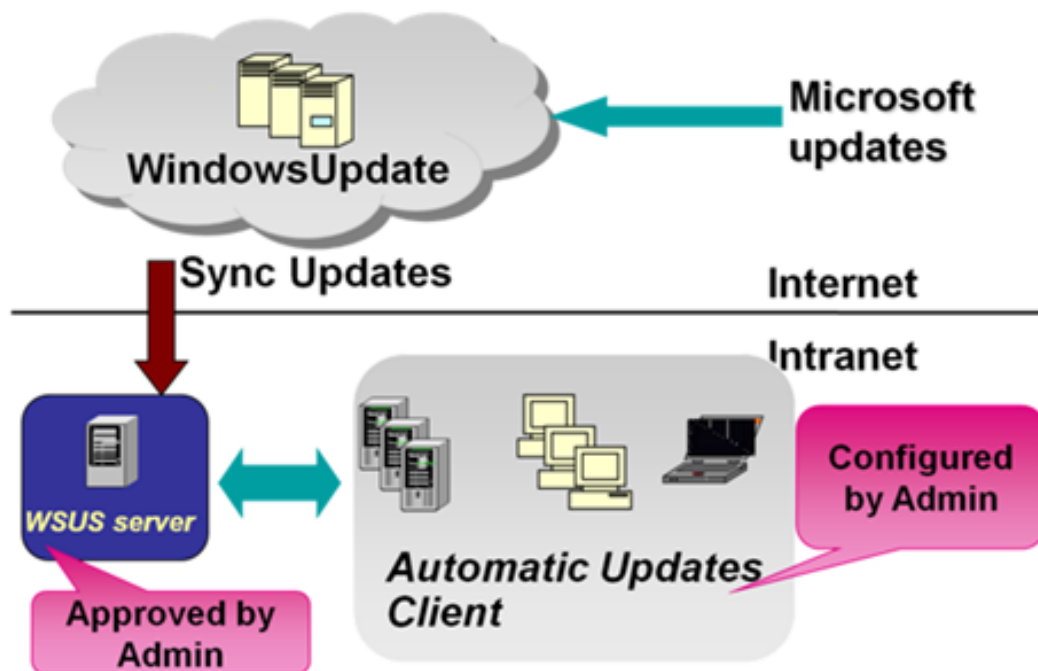
SVP support

- [Security patch and antivirus software policy](#)
- [Maintenance process](#)
- [Powering off the SVP](#)
- [Rebooting the SVP](#)
- [Backing up the SVP configuration](#)
- [Restoring the SVP configuration](#)
- [Changing the SVP IP address](#)
- [Deleting the registered storage system](#)
- [Registering the storage system on the SVP](#)
- [Blocking communications to port 80](#)

Security patch and antivirus software policy

ITPD provides HDS with recommended security and antivirus software information through ECNs. Users perform the necessary security measures by applying security patches, installing antivirus software, and turning-on automatic Windows update.

Windows Embedded Standard (WES) 7 provides the same look and feel, desktop environment, and security level as Microsoft Windows7 Professional. WES 7 also provides the same online and offline security-update methods as Microsoft Windows 7 Professional. Users apply security patches using a Windows Server Update Services server. Users can also apply security patches using a Windows Server Update Services server.



ITPD supports the following antivirus software applications:

- Trend Micro OfficeScan Corporate Edition 10.6
- Symantec Endpoint Protection 12.1
- McAfee VirusScan Enterprise 8.8
- Sophos Endpoint Security and Control 10.3

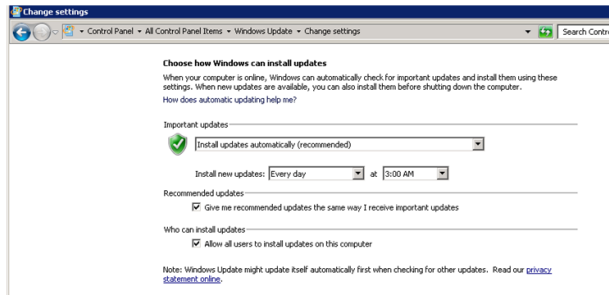
For more information, see:

- [HTTP://BLOGS.MSDN.COM/B/WINDOWS-EMBEDDED/ARCHIVE/2008/12/23/UPDATING-WINDOWS-EMBEDDED-STANDARD-SYSTEMS-USING-WSUS.ASPX](http://blogs.msdn.com/b/windows-embedded/archive/2008/12/23/Updating-Windows-Embedded-Standard-Systems-Using-WSUS.aspx)

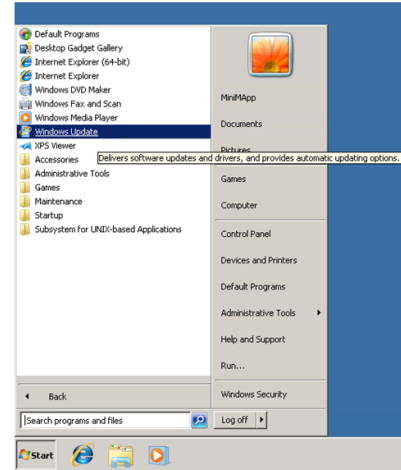
- [HTTP://DOWNLOAD.MICROSOFT.COM/DOWNLOAD/8/6/2/862977E5-8D21-4A1C-8DC9-C2289244C14C/WHAT'S%20NEW%20WITH%20SERVICING%20IN%20WINDOWS%20EMBEDDED%20STANDARD%207.PDF](http://download.microsoft.com/download/8/6/2/862977E5-8D21-4A1C-8DC9-C2289244C14C/WHAT'S%20NEW%20WITH%20SERVICING%20IN%20WINDOWS%20EMBEDDED%20STANDARD%207.PDF)

Online update

Users with storage systems in an online environment can apply security patches using automatic or manual "Windows Update."



OR

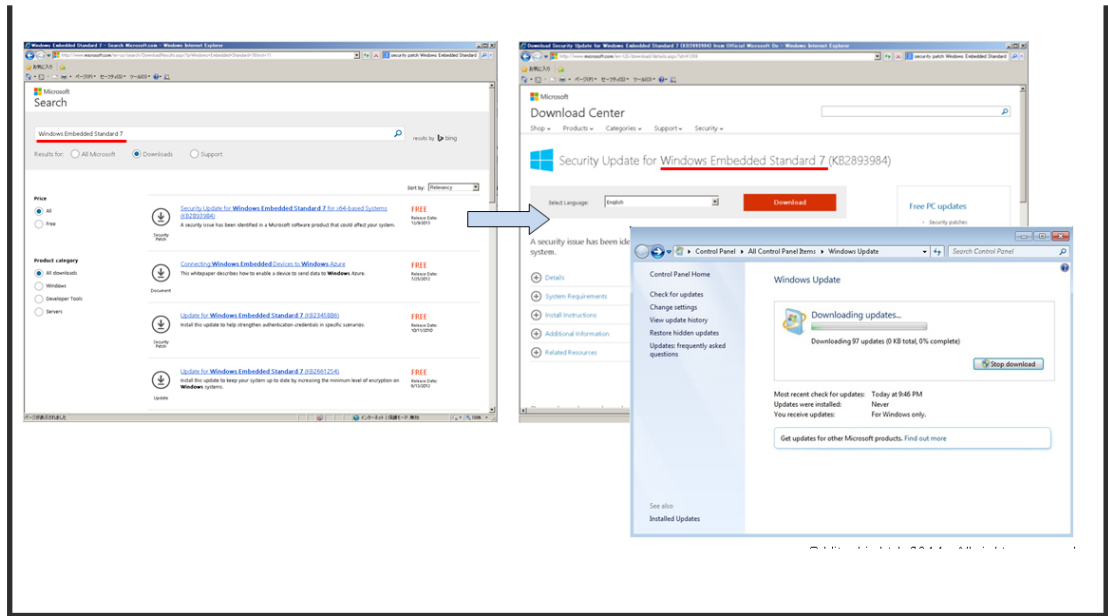


Offline update

User can apply Microsoft Windows Embedded Standard 7 security patches by downloading stand-alone packages from a Microsoft download site.

[HTTP://WWW.MICROSOFT.COM/EN-US/SEARCH/DOWNLOADRESULTS.ASPX?Q=WINDOWS+EMBEDDED+STANDARD+7&FIRST=11](http://www.microsoft.com/en-us/search/downloadresults.aspx?Q=WINDOWS+EMBEDDED+STANDARD+7&FIRST=11)

[HTTP://WWW.MICROSOFT.COM/EN-US/DOWNLOAD/DETAILS.ASPX?ID=41269](http://www.microsoft.com/en-us/download/details.aspx?id=41269)



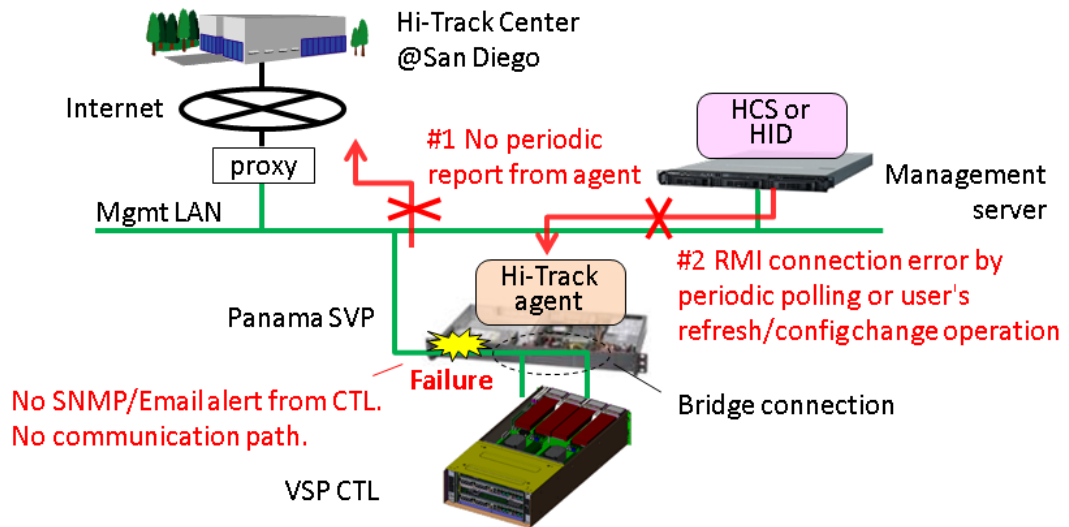
Maintenance process

The following sections describe the SVP maintenance process from failure detection to SVP recovery.

SVP failure detection

SVP failures are detected using the following methods:

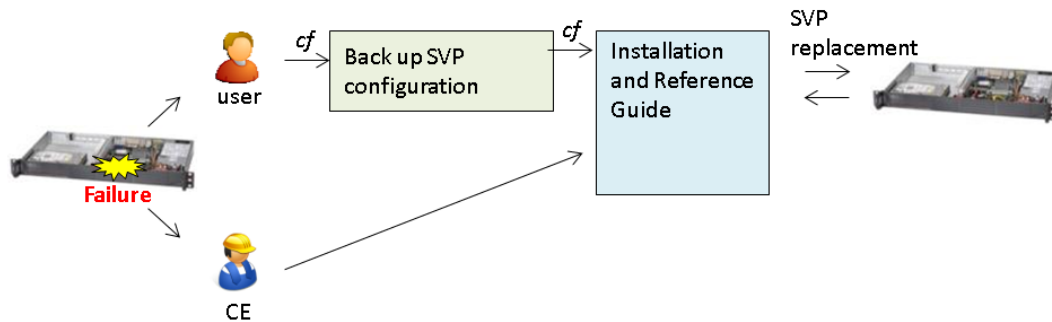
Fault detection method	How fault is detected	Action to be taken
Hi-Track Remote Monitoring System	No report from the agent during a 24-hour health check.	Hi-Track detects SVP failure -> SVP replacement.
Hitachi Command Suite	RMI connection error (not alert).	Refer to the Hitachi Command Suite Administrator Guide.
Infrastructure Director		



FRU replacement

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

The procedures for backing up and restoring the SVP configuration are in the *Hitachi VSP Hardware Reference Guide*.



Operating system recovery

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

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

Backing up the OS

Procedure

1. Boot the SVP.
2. When the Basic Input/Output System (BIOS) screen appears, press F8.
3. Select a partition for the backup.
4. Exit the BIOS and reboot the SVP.

Restoring the OS

Procedure

1. Boot the SVP.
2. When the BIOS screen appears, press F8.
3. Select an image to restore.
4. Exit the BIOS and reboot the SVP.

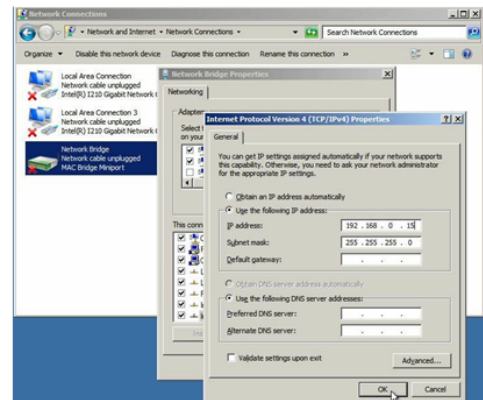
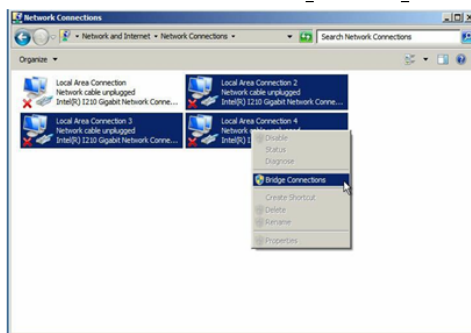
Creating a network bridge

When referring to the SVP, a "network bridge" refers to configuring the four SVP LAN ports for communication on a network.

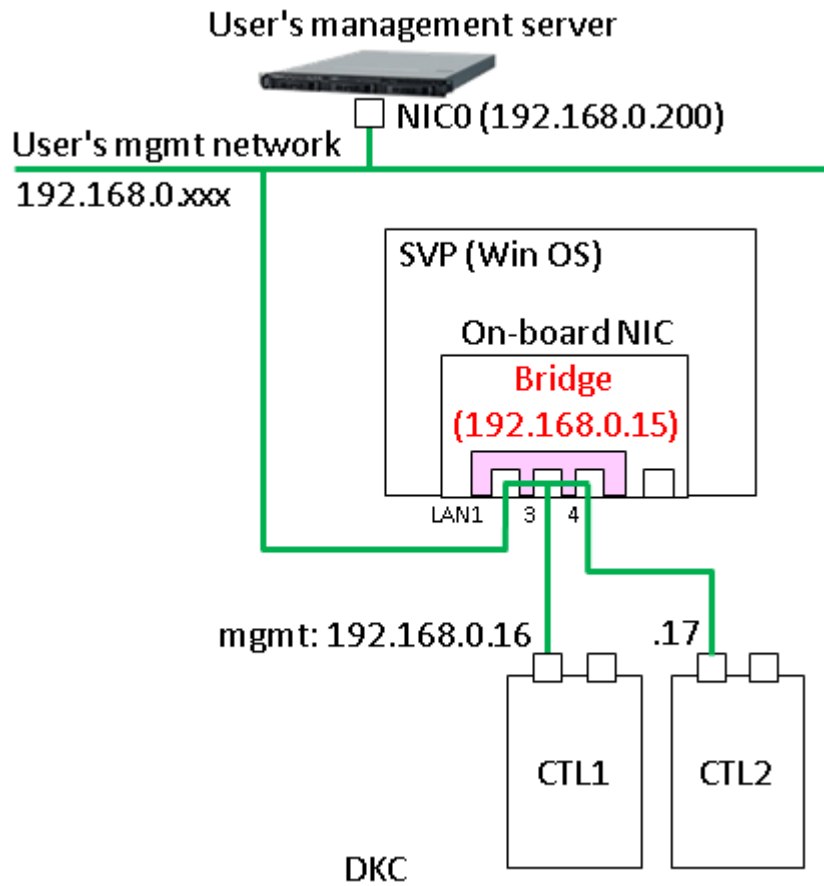
Procedure

1. In the SVP Windows Control Panel, click **Network and Sharing Center**.
2. In the right pane, click **Change adapter settings**.
3. Before configuring a bridge, delete all network setting for the three NICs you want to bridge.
4. Select the three NICs you want to bridge, and then right-click and click **Bridge Connections**.

A new instance of the network bridge appears.



- Assign the IP address 192.168.0.15 to the network bridge.



Powering off the SVP

Procedure

- From a management console PC, connect to the SVP using Windows Remote Desktop Connection.
- On the SVP, click **Start** in Windows desktop.
- From the displayed menu, click **Windows Security**.
- In the **Windows Security** window, click the option in the power (up arrow) menu.
- From the displayed menu, click **Shut down**.
The SVP power and `POWER` LED go off.

Rebooting the SVP

Procedure

1. From a management console PC, connect to the SVP using Windows Remote Desktop Connection.
2. On the SVP, click **Start** in Windows desktop.
3. From the displayed menu, click **Windows Security**.
4. In the **Windows Security** window, click the up arrow option in the power menu:



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

Backing up the SVP configuration

In the unlikely event the SVP fails and needs to be replaced, back up the SVP configuration file to a USB flash drive before returning the failed SVP. When you receive the replacement SVP, you can use the USB flash drive to restore the previous configuration on the new SVP. This procedure assumes that the client PC is connected to the SVP using a Remote Desktop connection.

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

- Parameters set in the Hitachi 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) in Device Manager - Storage Navigator
- Warning message in the Device Manager - Storage Navigator login window
- Device Manager - Storage Navigator task information
- SMI-S application settings
- HTTPS and SMI-S SSL certificates, and RM

To back up the SVP configuration:

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]
```
5. When the completion message appears, 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.

This procedure assumes that:

- The client PC is connected to the SVP using a Remote Desktop Connection.
- The storage system you want to restore is registered on the SVP.
- The service setting is configured to not start automatically when the SVP reboots.

To restore the SVP configuration:

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]
```
4. When the restoration message appears, press any key to continue.
5. Exit the command prompt.
6. Attach a USB flash drive to a USB port on the SVP, and then move the backup file from the SVP to the USB flash drive.
7. Configure the service setting to start automatically the next time the SVP reboots, and then reboot the SVP.

Changing the SVP IP address

You can change the IP address for the SVP using the Microsoft Windows Embedded Standard 7 operating system on the SVP or the Storage Device List.

Changing the SVP IP address in Windows 7

Use this procedure so long as no storage system has been registered on the SVP, or the storage system service has not been started.

Procedure

1. From a management console PC, connect to the SVP using Windows Remote Desktop Connection.
2. On the SVP, click **Start > Control Panel Network and Sharing Center**.
3. Click **Change adapter settings**.
4. Click a network for which you want to set an IP address, and then set the IP address.

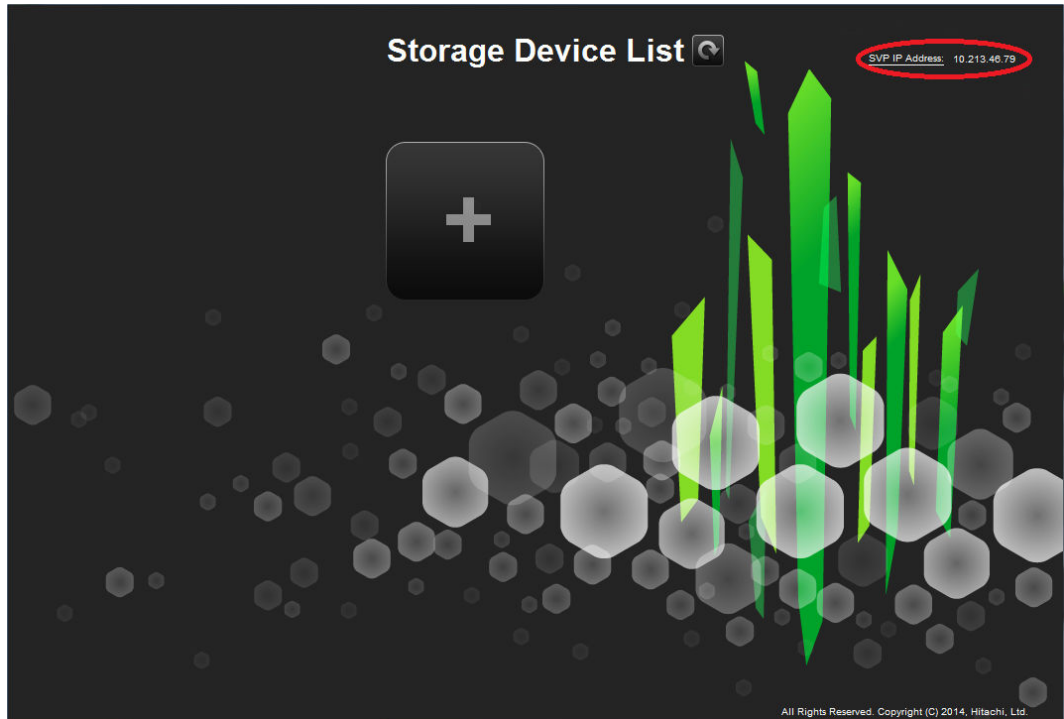
Changing the SVP IP address using the Storage Device List

To use this procedure, there must be no storage system registered on the SVP or the storage system service must not have been started.

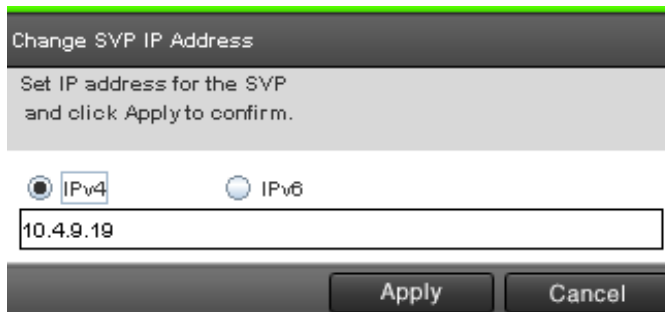
Procedure

1. If you have not connected a management console PC to the SVP using Windows Remote Desktop Connection, do so now.
2. On the SVP, click **Start > All Programs > Hitachi Device Manager-Storage Navigator > StorageDeviceList**.
The **Storage Device List** window opens.

3. Click **SVP IP Address** at the top-right side of the window.



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



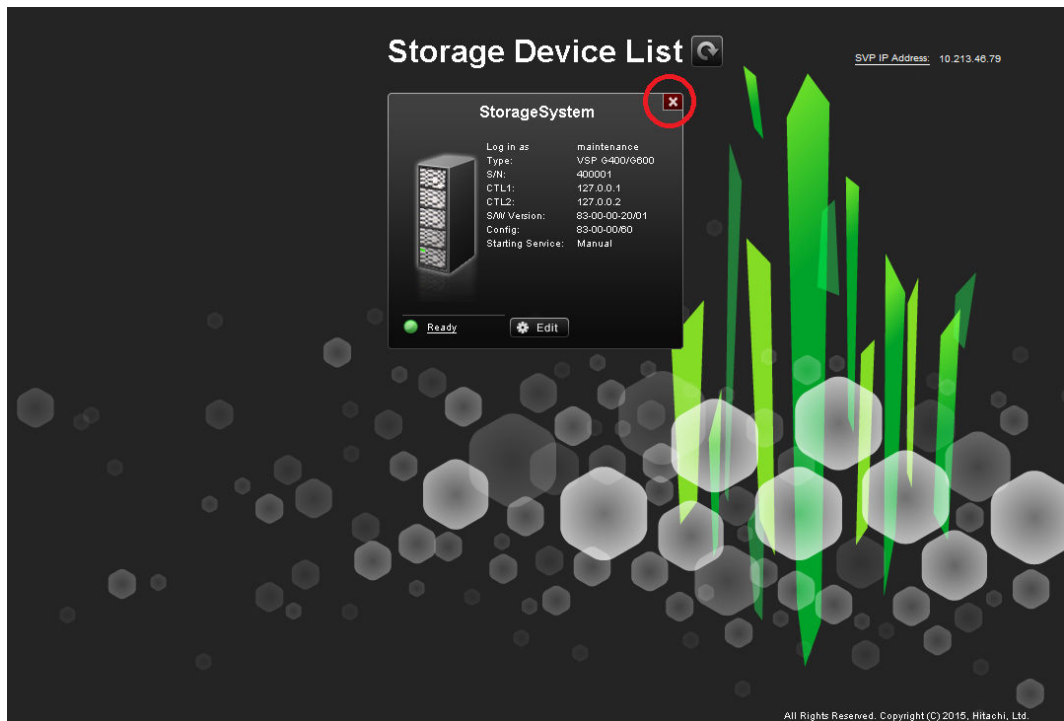
4. Click an IP addressing method (**IPv4** or **IPv6**).
5. Enter the new IP address of the SVP.
6. Click **Apply**.

Deleting the registered storage system

Use the following procedure in the unlikely event you need to delete the registered storage system from the SVP.

Procedure

1. From a management console PC, connect to the SVP using Windows Remote Desktop Connection.
2. Stop the SVP service (see [Stopping the SVP service](#)).
3. On the SVP desktop, double-click the **Open StorageDeviceList** icon. The **Storage Device List** window opens.
4. In the **Storage Device List** window, click **x** for the storage system that you want to delete.



Registering the storage system on the SVP

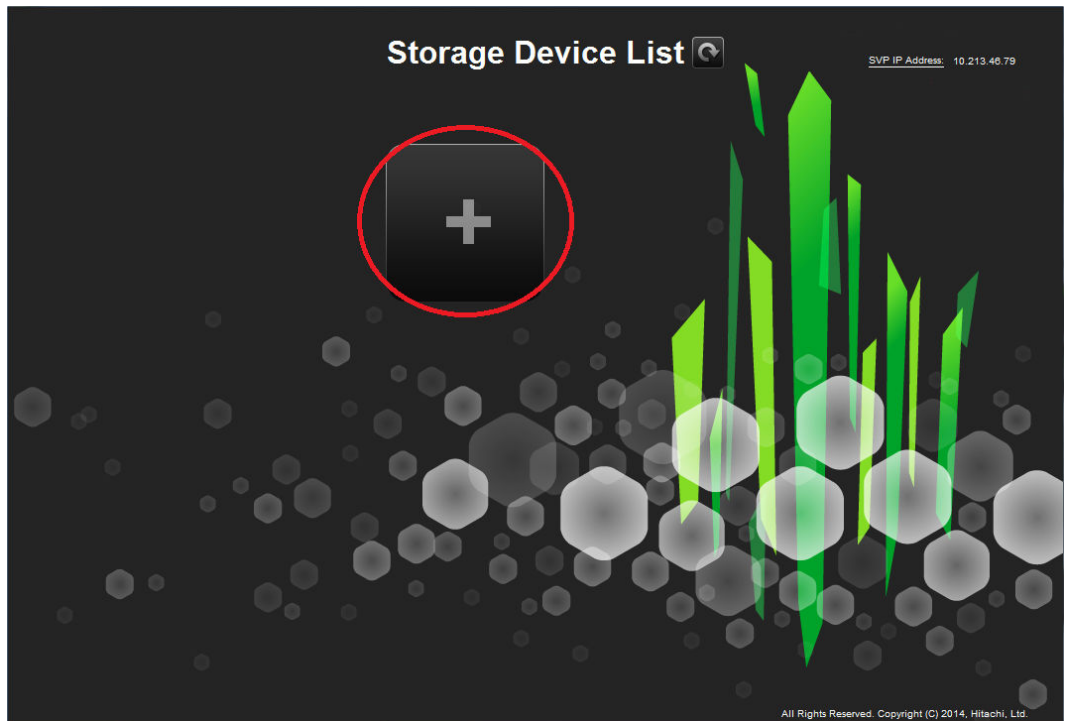
If you delete the registered storage system from the SVP, use this procedure to register the storage system with the SVP.

You register the storage system using the Storage Device List.

Procedure

1. From a management console PC, connect to the SVP using Windows Remote Desktop Connection.
2. On the SVP, click **Start > All Programs > Hitachi Device Manager-Storage Navigator > StorageDeviceList**.

3. Click the plus sign in the center of the window.
The **Add System** window appears.



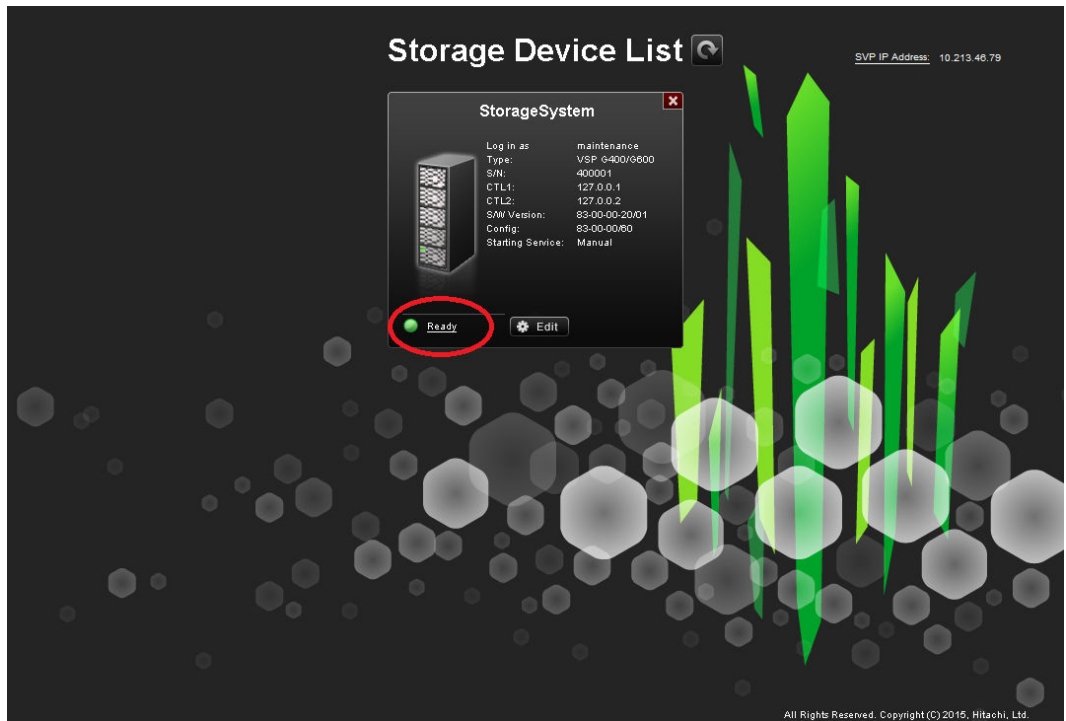
4. Complete the fields in the **Add System** window.

Field	Description
Software Selection	Click Browse and select the installation media, which ends in a .inf extension.
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

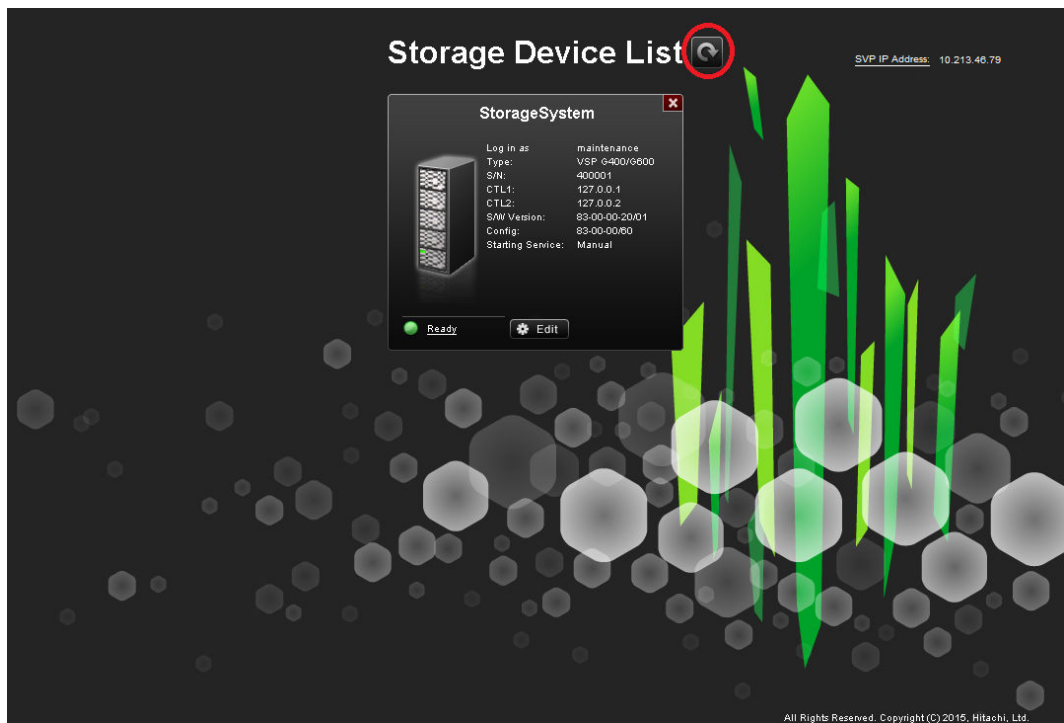
Field	Description
	then enter the IP address in the appropriate format for the addressing method selected.
System Name	Enter the display name of the storage system, up to 180 characters.
Description	Enter the description of the storage system, up to 180 characters.
User Name	Enter a user name, up to 256 characters. Permitted characters are alphanumeric characters and the following: (# \$ % & ' * + - . / = ? @ ^ _ ` { } ~)
Password	Enter a password, from 6 to 256 characters.

5. Click **Apply**.
The confirmation window appears and the registered storage system appears in the **Storage Device List** window.
6. Reboot the SVP (see [Rebooting the SVP on page 44](#)).
7. After the SVP reboots, click **Start > All Programs > Hitachi Device Manager-Storage Navigator > StorageDeviceList**.

8. Wait for the storage system status becomes **Ready**.



Note: If the storage system status does not become **Ready**, click **Refresh**.



If an error message appears, see [Troubleshooting Storage Navigator](#).

Blocking communications to port 80

The following procedure describes how to block HTTP communications to the SVP using port 80.

Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
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 block file exists, and then issue the following command:

```
C:\MAPP\wk\Supervisor\MappIniSet\MappHttpBlock.bat
```
5. When the completion message appears, press any key to continue.
6. Exit the command prompt.

Postrequisites

To unblock port 80, repeat this procedure, but issue the following command in step 3:

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


Hitachi Data Systems

Corporate Headquarters

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

Regional Contact Information

Americas

+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa

+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific

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



FE-94HM8036-00