

Hitachi Virtual Storage Platform Fx00 and Gx00

Service Processor Technical Reference

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

© 2015, 2018 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 copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

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

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

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

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

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

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

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

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft 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 website are properties of their respective owners.

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	9
Intended audience	9
Document conventions	9
Changes in this revision	
Conventions for storage capacity values	
Accessing product documentation	
Getting help	
Comments	12
Chapter 1: SVP overview	13
Chapter 2: Physical SVP (Windows 7) hardware description	17
SVP front panel	17
SVP rear panel	18
Service processor (Windows 7) hardware specifications	18
Physical SVP (Windows 7) electrical specifications	19
Physical SVP (Windows 7) environmental specifications	20
Chapter 3: Physical SVP (Windows 10 Enterprise) hardware description.	າາ
SVP front panel SVP rear panel	
Service Processor (Windows 10 Enterprise) hardware specifications	
Physical SVP (Windows 10 Enterprise) electrical specifications	
Physical SVP (Windows 10 Enterprise) environmental specifications	
Chapter 4: Installing the Hitachi Vantara-supplied SVP	
Physical SVP network configuration	
Physical SVP LAN port assignment	
Default IP address settings	
Installing a physical SVP	
Mounting the physical SVP	
Choosing a mounting location	
Installing the inner rail extension	
Installing the outer rails to the rack	31
Installing the physical SVP into the rack	

Contents

Connecting to the physical SVP	33
Turning on power to the physical SVP	34
Operating the physical SVP in a non-bridged network configuration	35
Setting the SVP date, time, and time zone settings	37
Disconnecting the management console from the physical SVP	43

Minimum requirements for installing the SVP software on customer-	
supplied server	
Setting up the SVP locale	
Configuring the operating system	45
Logging on to the operating system	45
Configuring the Control Panel display	
Configuring the desktop	46
Configuring the task bar and the start menu properties	47
Configuring the time settings	
Configuring region settings	53
Configuring the power management settings	
Configuring Action Center settings	
Configuring the troubleshooting settings	61
Configuring the Remote Desktop settings	
Configuring Internet Explorer settings	
Disabling the auto-execute feature	
Configuring the Registry	72
Enabling ICMP (ping) reply	
Changing the computer name	
Changing the account name	
Configuring the password setting for Administrator	
Changing the password setting	
Configuring Internet Information Services	
Installing the SVP software	

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

hos	st	100
	Physical network connection for an Oracle Linux KVM-based SVP	100
	Minimum requirements for an Oracle Linux KVM SVP	101
	Hyper-threading	102
	Configuring the Oracle Linux KVM-based SVP	103
	Where to go from here	106
~		

Chapter 7: Installing the SVP software on a VMware ESXi host.... 107

Setting up the SVP locale10	7
-----------------------------	---

Contents

Network connection for virtual SVP	107
Virtual SVP requirements	
Hyper-threading	109
Configuring the virtual SVP	109
Configuring the SVP guest OS	112
Logging on to the operating system	112
Configuring the Control Panel display	113
Configuring the desktop	113
Configuring the task bar and the start menu properties	115
Configuring the time settings	120
Configuring region settings	121
Configuring the power management settings	124
Configuring Action Center settings	127
Configuring the troubleshooting settings	129
Configuring the Remote Desktop settings	
Configuring Internet Explorer settings	132
Disabling the auto-execute feature	
Configuring the Registry	140
Enabling ICMP (ping) reply	
Changing the computer name	146
Changing the account name	
Configuring the password setting for Administrator	
Changing the password setting	
Installing the SVP software	
Deploying a cloned virtual SVP	
Detecting SVP failures	166

Setting up the SVP locale	168
Network connection for Hyper-V	168
Minimum requirements for Hyper-V Server 2012 R2 VM	169
Installing and Configuring Hyper-V on Windows 2012 R2 Server	170
Installing the SVP software on a guest OS	171
Chapter 9: Upgrading the SVP software	.176
Stopping the service in each storage system	176
Upgrading the SVP software only	177
Upgrading the storage management, SVP software, and storage system	
firmware	182
Stopping the SVP service	189
Upgrading the SVP software using Storage Device List	190

Downgrading the SVP software	193
Chapter 10: Security patch and antivirus software Online update Offline update Installing antivirus software on the SVP	194 195
Chapter 11: Setting up SSL encryption	
About SSL	
SSL encryption of the storage system	
Setting up SSL communications Updating the SVP server certificate	
Creating a private key (.key file)	
Creating a public key (.csr file)	
Acquiring a signed certificate for the private key	
Acquiring a signed and trusted certificate	
Removing the passphrase from an SSL certificate	
Converting the SSL certificate into the PKCS#12 format	203
Uploading the signed server certificate of the SSL communication between the SVP and client PC	
Returning the certificate of the SSL communication between the SVP and the client PC to the default	204
Uploading the certificate to the SVP	
Uploading the certificate to the web server	
Returning the web server certificate to the default	
Resolving security certificate messages	
Blocking HTTP communications to the SVP	207
Releasing HTTP communications to the SVP	208
Chapter 12: Changing the storage IP address	. 209
Using the SVP to set the storage system IP address	
Changing storage system information in the Storage Device List	
Chapter 13: Changing the SVP IP address	.212
Changing the SVP IP address in Windows 7	
Changing the SVP IP address using Storage Device List	
Chapter 14: Changing and initializing SVP port numbers	. 214
Changing SVP port numbers	
Initializing SVP port numbers	
Behavior when changing SVP port numbers	219
Reallocating automatically allocated port numbers	221
Initializing automatically allocated port numbers	
Changing range of port numbers to be allocated automatically	223

Contents

Initializing range of port numbers to be allocated automatically Viewing the port number to be used in the SVP	
Chapter 15: Editing the Storage Device List	227
Chapter 16: Deleting and registering the storage system	236
Deleting the registered storage system from the Storage Device List	.236
Registering the storage system on the SVP	. 237
Chapter 17: Back up and restore the SVP	248
Backing up the SVP configuration	. 248
Restoring the SVP configuration	249
Chapter 18: Rebooting the SVP	250
Shutting down the SVP	
Restarting the SVP	. 250
Chapter 19: Replacing the Hitachi Vantara-supplied SVP	.251
Detecting SVP failures	054
	.251
Replacing the physical SVP	
Replacing the physical SVP Recovering the operating system	252 . 252
Replacing the physical SVP Recovering the operating system Backing up the OS	252 . 252 . 253
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS	252 . 252 . 253 253
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP	252 . 252 . 253 253 253 . 253
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP Mapping the internal SVP network adapters	252 . 252 . 253 253 . 253 . 253 . 253
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP Mapping the internal SVP network adapters Renaming the internal SVP network adapters	252 . 252 . 253 253 . 253 . 253 . 254
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP Mapping the internal SVP network adapters Renaming the internal SVP network adapters Setting the IP address	252 . 252 . 253 253 . 253 . 253 . 253 . 254 . 255
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP Mapping the internal SVP network adapters Renaming the internal SVP network adapters Setting the IP address Configuring bridge settings	252 . 252 . 253 . 253 . 253 . 253 . 254 . 255 256
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP Mapping the internal SVP network adapters Renaming the internal SVP network adapters Setting the IP address	252 . 252 . 253 . 253 . 253 . 253 . 254 . 255 256
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP Mapping the internal SVP network adapters Renaming the internal SVP network adapters Setting the IP address Configuring bridge settings	252 . 252 . 253 . 253 . 253 . 253 . 253 . 254 . 255 256 266
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP Mapping the internal SVP network adapters Renaming the internal SVP network adapters Setting the IP address Configuring bridge settings Installing Hitachi Device Manager - Storage Navigator	252 . 252 . 253 . 253 . 253 . 253 . 253 . 254 . 255 256 256 266 272
Replacing the physical SVP Recovering the operating system Backing up the OS Restoring the OS Configuring the replacement physical SVP Mapping the internal SVP network adapters Renaming the internal SVP network adapters Setting the IP address Configuring bridge settings Installing Hitachi Device Manager - Storage Navigator	252 . 252 . 253 . 253 . 253 . 253 . 253 . 255 256 266 272 272

Preface

Intended audience

This document is intended for Hitachi Vantara representatives and authorized service providers who install, configure, or operate storage systems.

This document is intended for customers inquiring about the features and specifications of the storage system.

Readers of this document should be familiar with the following:

- Data processing and RAID storage systems and their basic functions.
- 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 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 <i>group</i>
		(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	Indicates variables in the following scenarios:	
brackets	 Variables are not clearly separated from the surrounding text or from other variables. Example: 	
	Status- <report-name><file-version>.csv</file-version></report-name>	
	 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:

lcon	Label	Description
	Note	Calls attention to important or additional information.
0	Тір	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

- Added physical, electrical, and environmental specifications for new service processor hardware with Microsoft Windows 10 Enterprise.
- Updated diagrams in Operating the physical SVP in a non-bridged network configuration.

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: <u>https://knowledge.hitachivantara.com/Documents</u>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

<u>Hitachi Vantara Support Connect</u> 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: <u>https://support.hitachivantara.com/en_us/contact-us.html</u>.

<u>Hitachi Vantara Community</u> 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 <u>community.hitachivantara.com</u>, register, and complete your profile.

Comments

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

Thank you!

Chapter 1: SVP overview

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

The SVP is available as a physical (bare-metal) 1U management server or as a 64-bit software application provided by Hitachi Vantara. The physical SVP server and the SVP software applications are supported in the environments shown in the following table.

For the latest interoperability updates and details, see the *SVP* (*Service Processor*) *OS* and *Hypervisor support for Gx00, Fx00* report at <u>https://support.hitachivantara.com/en_us/</u><u>interoperability.html</u>.

Operating system	Server/virtual machine	Minimum SVP version	Notes and additional requirements
Windows 7	VMware ESXi 6.0.0	88-01-02-x0/00	-
Professional	KVM on Oracle Linux 7.2	88-01-02-x0/00 ¹	
	(3.8.13-98.7.1.el7ue k.x86_64, qemu- kvm-1.5.3-105.el7.x 86_64)		
Windows 7 Professional Service Pack 1	VMware ESXi 6.0.0(Update 2) Cluster	88-01-02-x0/00 ¹	-
Windows 2012 r2	Microsoft Hyper-V Server 2012 R2	88-01-02-x0/00 ¹	-
Windows 10 Enterprise	Microsoft Hyper-V Server 2012 R2	88-01-02-x0/00 ¹	-
Note:	1	1	I

Table 1 Service processor (with Windows 10 Enterprise)

Note:

¹"x" of SVP version shows model, '6' is "VSP G900 and VSP F900" or "VSP G700 and VSP F700" or "VSP G370 and VSP F370, '2' is "VSP G350 and VSP F350".

Operating system	Server/virtual machine	Minimum SVP version	Notes and additional requirements
Windows 7 Professional	Bare metal installation (see requirements)	83-01-03-x0/00	-
	VMware ESXi 6.0.0	83-03-02-x0/00	-
	KVM on Oracle Linux 7.2	83-03-23-x0/00	OS kernel version for Oracle Linux: 3.8.13-98.7.1.el7uek.x8 6_64
			OS kernel version for KVM: qemu- kvm-1.5.3-105.el7.x86_ 64
Windows 7 Professional Service Pack 1	VMware ESXi 6.0 U2	83-03-23-x0/00	Cluster is supported.
Windows Server 2012	Bare metal installation (see requirements) VMWare ESXi 6.0 U2	83-01-03-x0/00	-
Windows Server 2012 R2	Bare metal installation (see requirements)	83-01-03-x0/00	-
	Hyper-V Server 2012 R2	83-04-02-x0/00	-
	VMWare ESXi 6.0 U2		
Windows 10 Professional	Bare metal installation (see requirements)	83-04-02-x0/00	-
Windows 10 Enterprise	Bare metal installation (see requirements)	83-04-02-x0/00	-
	Microsoft Hyper-V Server 2012 R2		
Windows Server	Bare metal	83-04-27-x0/00	-
2016	installation (see requirements)	83-04-47-x0/00	-

Table 2 Service processor (with Windows 7)

Chapter 1: SVP overview

The bare metal servers must meet the following requirements.

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

The following table lists SVP VM requirements.

VM platform	Requirements	Corresponding SVP guest OS
ESX Server	VMware ESXi server 6.0	SVP Guest OS (maximum one DKC per SVP guest OS)
	Two quad core processors, Intel Xeon 2.29 GHz	Two virtual CPUs
	One port network interface card (NIC)	One virtual network adapter
	32 GB RAM	4 GB RAM
		120 GB disk space
Linux KVM Server	Oracle Linux 7.2	Same as ESX Server
	Two quad core processors, Intel Xeon 2.29 GHz	
	One-port NIC	
	128 GB RAM	
Hyper-V Server	Hyper-V server 2012 R2	Same as ESX Server
	Two quad core processors, Intel Xeon 2.29 GHz	
	One port NIC	
	32 GB RAM	

Chapter 1: SVP overview



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

Chapter 1: SVP overview

Chapter 2: Physical SVP (Windows 7) hardware description

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

SVP front panel

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

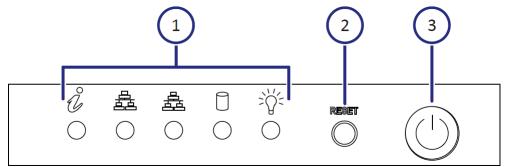


Table 3 SVP (Windows 7) front panel

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 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.

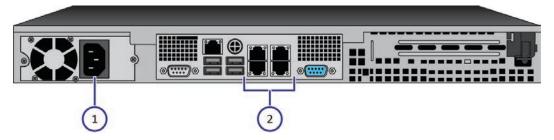


Table 4 SVP (Windows 7) rear panel

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.

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

Service processor (Windows 7) hardware specifications

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



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

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

Physical SVP (Windows 7) electrical specifications

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

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

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

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

VA is 140.69, with a 0.8 power factor.



Note: The measurements are not kilo values.

Physical SVP (Windows 7) environmental specifications

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

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

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

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

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

SVP front panel

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



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		

Table 5 SVP (Windows 10 Enterprise) front panel

SVP rear panel

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

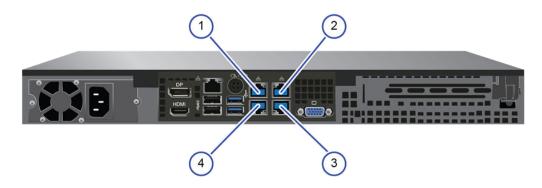


Table 6 SVP (Windows 10 Enterprise) rear panel

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

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

Note: After the Initial Startup Wizard is complete, the SVP can be used in nonbridge 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		
LAN/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 supplied 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	e humidity range 8% ~ 90% (non-condensing)	
Non-operating relative humidity range	midity range 5% - 95% (non-condensing)	

Chapter 4: Installing the Hitachi Vantarasupplied SVP

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

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



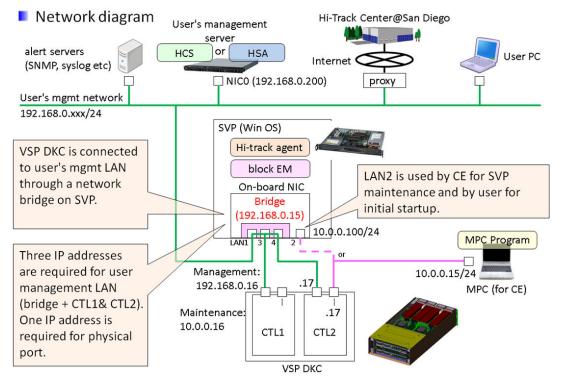
Important: The Hitachi Vantara-supplied SVP can only be installed, upgraded, or replaced by a Hitachi Vantara representative or an authorized service provider. Contact a Hitachi Vantara representative for more information about installing, upgrading, or replacing a Hitachi Vantara-supplied SVP.

Physical SVP network configuration

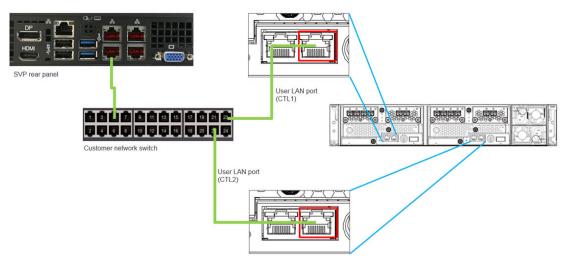
In networking terms, a *network bridge* is software or hardware that connects two or more networks so that they can communicate. For the physical SVP, a network bridge configures the three local-area network (LAN) ports on the SVP using the Bridge Connections setting in the Windows operating system.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

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

Note: The Hitachi Vantara-supplied 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 the storage array being managed if they belong to the same subnet.



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

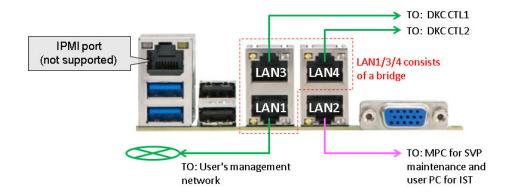


For information about configuring an SVP for a non-bridged network environment, see <u>Operating the physical SVP in a non-bridged network configuration (on page 35)</u>.

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 is invisible from the Windows operating system. For security reasons, the IPMI port cannot be enabled in BIOS setting and is not supported for the SVP.



Default IP address settings

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

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

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	10.0.0.100/2 4	<	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 high-temperature environments. Do not operate the SVP at temperatures above 95°F (35°C).

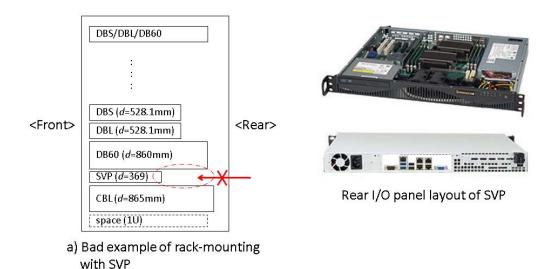


Caution: The SVP (Windows 10) is supported in high-temperature environments. Do not operate the SVP at temperatures above 104°F (40°C).

Mounting the physical SVP

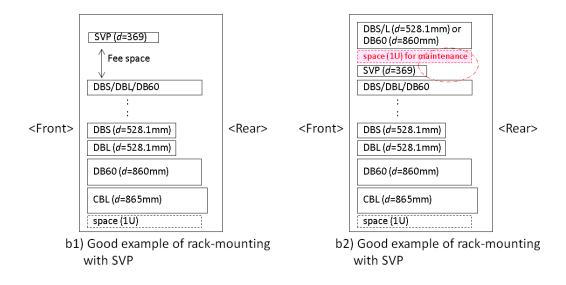
The physical SVP has a depth of 14.5 inches (369 mm). The 4U CBL controller and dense intermix drive tray (DB60) have a depth of 34.1 inches (865 mm) and 33.9 inches (860 mm), respectively.

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



To verify 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.



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.

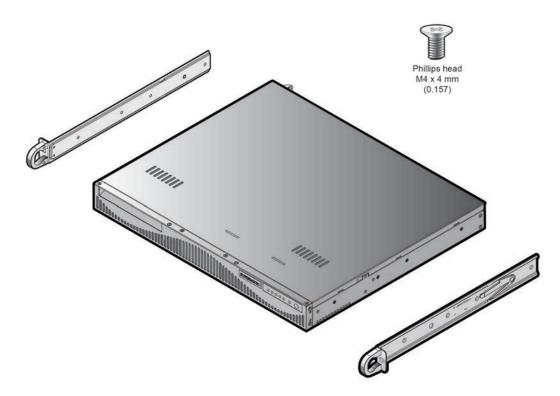
Installing the inner rail extension

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 with the other chassis ear.



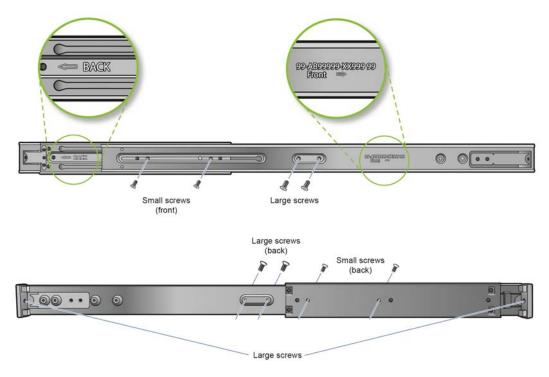
- **2.** Find the **Front** marking on the rails, and then orient the rails appropriately for attaching to the SVP chassis.
- **3.** Screw the internal racks onto the SVP chassis using the four large screws and the two small screws.
- **4.** Repeat steps 2 and 3 for the inner rail extension on the other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

- 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 that the front of the rail faces the front of the rack. Adjust both 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:

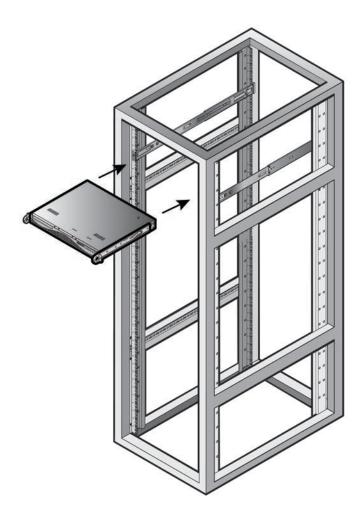
- The inner rails are attached to the SVP enclosure.
- The outer rails are attached to the rack.

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.

- SVP LAN3 Connected to user LAN port on Controller 1 Network Switch LAN2 Management Console PC
- 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: The creation of 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/).

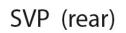
For more information, see the Service Processor Technical Reference.

Turning on power to the physical SVP

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

Procedure

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





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

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

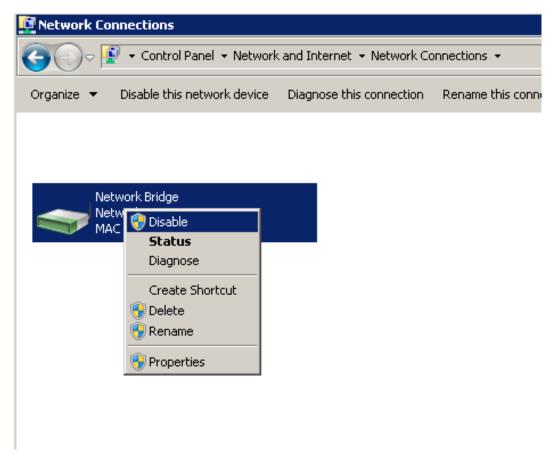
Operating the physical SVP in a non-bridged network configuration

If BPDU is enabled in your network environment, use the following 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 the Ethernet switch.

Procedure

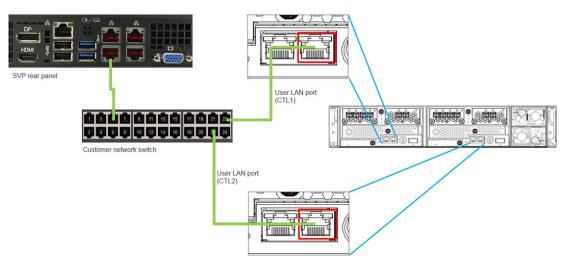
- **1.** Connect a PC to the LAN2 port on the SVP.
- **2.** Log on to the SVP using the Remote Desktop Connection:
 - a. Configure the PC to use an IP address of 10.0.0.xxx, where xxx = 1-99 or 101-254, and a subnet mask of 255.255.255.0.
 - b. Click **Start > All Programs**, and then select **Accessories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

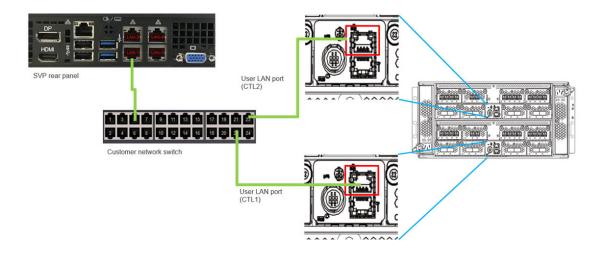


6. Remove the Ethernet cables from SVP ports LAN3 and LAN4, and attach them to the Ethernet switches.

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 the Windows 7 operating system running on the SVP, and then specify the same settings in the maintenance utility.

Before you begin

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

Procedure

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

📸 Date and Time	×
Date and Time Additional Clocks	Internet Time
	Date: Tuesday, March 24, 2015 Time: 12:28:42 AM S Change <u>d</u> ate and time
(UTC) Coordinated Universa	al Time
	Change time <u>z</u> one
Daylight Saving Time is not	observed by this time zone.
Get more time zone inform How do I set the clock and t	
	OK Cancel Apply

- 4. Click Change date and time.
- 5. Set the year, month, day, and time, and then click **OK**.

e:							Time:
1		Mar	ch, 2	015			North Party
ı	Mo	Tu	We	Th	Fr	Sa	-
2	23	24	25	26	27	28	
1	2	3	4	5	6	7	
3	9	10	11	12	13	14	
5	16	17	18	19	20	21	L'achara V
2	23	24	25	26	27	28	
9	30	31	1	2	3	4	12: 33: 17 AM

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

📽 Date and Time	×
Date and Time Additional Clo	cks Internet Time
	Date: Tuesday, March 24, 2015 Time: 12:28:42 AM () Change <u>d</u> ate and time
Time zone	
(UTC) Coordinated Unive	rsal Time Change time <u>z</u> one
Daylight Saving Time is n	ot observed by this time zone.
<u>Get more time zone infor</u> <u>How do I set the clock an</u>	
	OK Cancel Apply

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

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

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

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

Maintenance Utility		Alert System Unlocked	Logged in as: maintenance Log Out ?
Storage System	Date & Time		Last Updated : 2015/09/17 20:21 🔯
Ready	(Set Up)		
Serial Number : 407001 Connected to : CTL2 Hardware Administration • remware • Alex Notifications • Licenses • Network Settings • Date & Tom • Auto, cory settings	System Date & Time UTC Timezone Automatically adjust clock for Davlight Saving Time Use NTP Server NTP Server Synchronizing Time	2015/09/17 20:21 Kaload (GNT-09:00)Osaka/Sapporo/Tokyo · Yes ntp.nict.jp 09:00	
MCNU 61 Initial Setup Wizard 66 Power Management 61 System Management			

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

Set Up Date & 1	Time		
To set the date and tin When the settings are	ne of the system, specify t complete, verify the setting	he UTC Timezone, the NTP Server information, and S gs, and then click [Apply].	ynchronizing Time.
UTC Timezone:	(UTC-08:00)Pacific Time	(US & Canada)	
	Automatically adjust cl	lock for Daylight Saving Time	
Use NTP Server:	Yes: NTP Server:	ntp.nict.jp	
		+ Add NTP Server	
	◎ No: Date & Time:	2015/10/08 20 : 4	
Synchronizing Time:	16 : 0		
			Apply Cancel ?

Field	Descr	ription
UTC Time zone	Select a time zone on the Time map.	Coordinated Universal
Automatically adjust clock for Daylight Saving Time	This field is available only zone supports daylight sa option if your location ob time (also known as sumr	aving time. Check this serves daylight saving
Use NTP Server	Select an option for main utility time.	taining the maintenance
	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.

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

- d. Click **Apply**.
- e. In the confirmation message, click **Close**.

Disconnecting the management console from the physical SVP

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

Procedure

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



Result

The SVP disconnects from the PC.

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

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

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

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

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

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

Setting up the SVP locale

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

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

Configuring the operating system

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

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

Logging on to the operating system

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

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



Next steps

Configure the Control Panel display.

Configuring the Control Panel display

Procedure

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

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

Configuring the desktop

Configure the Windows screen saver function on the SVP.

Procedure

1. Click Control Panel > Personalization. For Basic and High Contrast Themes (6), click Windows Classic.



- 2. Click Screen saver.
- 3. In Screen saver, click Blank, and then set Wait to 60 (minutes).
- **4.** Click **OK**.

and the second h			
reen Saver			
		.0	
Screen saver		1	
Screen saver	_	Settings	Preview
Blank	.		
Blank	▼ inutes 「 On resur		
Blank Wait: 60 🛨 m	▼ inutes 「 On resur		
Blank Wait: 60 🛨 m Power management		me, display logon	screen
Blank Wait: 60 🛨 m	naximize performa	me, display logon	screen
Blank Wait: 60 1 m Power management Conserve energy or r brightness and other	naximize performa power settings.	me, display logon	screen
Blank Wait: 60 🛨 m Power management Conserve energy or r	naximize performa power settings.	me, display logon	screen
Blank Wait: 60 1 m Power management Conserve energy or r brightness and other	naximize performa power settings.	me, display logon	screen

Next steps

Configure the task bar and the start menu properties.

Configuring the task bar and the start menu properties

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

Procedure

- 1. Click Control Panel > Taskbar and Start Menu Properties (task bar property), and then click the Taskbar tab.
- 2. Click Customize.

Taskbar appearance	
Lock the taskbar	
Auto-hide the taskbar	
Use small icons	
Taskbar location on screen:	Bottom
Taskbar buttons:	Always combine, hide labels 💌
notification area.	
Preview desktop with Aero Pe	ek
Temporarily view the desktop Show desktop button at end o	when you move your mouse to the
where aconcep parcent at cita a	
Use Aero Peek to preview.	
Vise Aero Peek to preview	an na ana sa

3. In the Notification Area Icons window, check Always show all icons and notifications on the taskbar.

- Control Panel - All Control Panel Items - Notification	on Area Icons	- 🔛	Search Control Panel	
Select which icons and notifications appear on the If you choose to hide icons and notifications, you won't click the arrow next to the notification area on the tasks	be notified about changes or	updates. To	o view hidden icons at any	time,
Icons	Behaviors			-
Action Center Solve PC issues: 2 important messages	Show icon and not	ifications	÷.	
Network Not Connected You are currently not co	Show icon and not	ifications		
Volume No Audio Output Device is installed.	Show icon and not	ifications	*	
Windows Explorer Safely Remove Hardware and Eject Me	Only show notifica	tions	Ŧ	_
Windows host process (Rundll32)	Only show notifica	tionș	*	-
Turn system icons on or off				
Restore default icon behaviors				
Always show all icons and notifications on the taskba	ar			

- **4.** Click **OK**.
- 5. Click Control Panel > Taskbar and Start Menu Properties (task bar property), and then click the Start Menu tab.
- 6. Click Customize.

askbar Start Menu	Toolbars	
To customize how links behave in the Start me	, icons, and menus look and enu, dick Customize.	Customize
Power button action:	Shut down	•
Privacy		
Store and display	recently opened programs	in the Start menu
Store and display	y recently opened items in th	e Start menu and
	and the second sec	
How do I change the v	vay the Start menu looks?	

7. In the Customize Start Menu window, check Run command and click Display on the All Programs menu and the Start menu.

O Display as a link	-
O Display as a menu	
 Don't display this item 	
Run command	
Search other files and libraries	
O Don't search	
 Search with public folders 	
 Search without public folders 	
Search programs and Control Panel	
Sort All Programs menu by name	
i System administrative tools	
O Display on the All Programs menu	
Display on the All Programs menu and the Start	menu
O Don't display this item	
Use large icons	
Videos	
O Display as a link	
Start menu size	
Number of recent programs to display:	10 🛨
Number of recent items to display in Jump Lists:	10 ÷

8. Under Music, check Don't display this item.

	O Display as a menu	10000
_	 Don't display this item 	
N	Enable context menus and dragging and dropping	
	Favorites menu	
8	Games	
	O Display as a link	
	O Display as a menu	
	O Don't display this item	
범	Help	-
넴	Highlight newly installed programs	
Ч	Homegroup	
ď	Music	
	O Display as a link O Display as a menu	
	 Display as a menu Don't display this item 	
	Network	
님	Open submenus when I pause on them with the mouse pointer	Î
Ľ	open submenus when I pause on them with the mouse pointer	10
Sta	art menu size	_
NU	Imber of recent programs to display:	-
-		
Nu	Imber of recent items to display in Jump Lists: 10 🚽	

- 9. Click OK.
- **10.** In the **Taskbar and Start Menu Properties** window, click **OK**.

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

Configuring the time settings

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

Procedure

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



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

Configuring region settings

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

Procedure

1. Click Control Panel > Region and Language, and then click the Keyboards and Languages tab.

mats	Location	Keyboards and	d Languages Administrative
Keybo	oards and	other input la	nguages
To ch	nange you	ir keyboard or	input language click Change keyboards.
			Change keyboards
How	do I chan	ge the keyboa	rd layout for the Welcome screen?
Displa	ay languag	ge	
			s that Windows can use to display text and speech and handwriting.
write	re suppor	ted recognize :	
			Install/uninstall languages
łow c	an I install	l additional lan	i <u>guages?</u>

- 2. Click Change keyboards.
- 3. In the Text Service and Input Languages window, click the Language Bar tab.
- 4. Click Hidden, and then click OK.

🧬 Region and Language	×
Formats Location Keyboards and Languages Administrative	
Services and Input Languages	×
General Language Bar Advanced Key Settings	
Language Bar C Eloating On Desktop C Docked in the taskbar C Hidden	
 Show the Language bar as transparent when inactive Show additional Language bar icons in the taskbar Show text labels on the Language bar 	
OK Cancel	Apply

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

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



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

Configuring the power management settings

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

Procedure

- Click Control Panel > Power Options, and then click the Show additional plans list.
- 2. Click Change settings that are currently unavailable.

🗲 🕞 - Control Panel + 🖌	I Control Panel Items · Power Options	- 🖾	Search Control Panel	1
Control Panel Home	51. s			6
	Select a power plan			
Choose what the power button does	Power plans can help you maximize your compu it, or choose a plan and customize it by changing	uter's performance or c ng its power settings. <u>1</u>	onserve energy. Make a ell me more about power	plan active by selecting plans
Create a power plan	Preferred plans			
Choose when to turn off the Balanced (recommended)			Ch	ange plan settings
display	Automatically balances performance	with energy consum	ption on capable hards	vare.
	Power saver		Ch	ange plan settings
	Saves energy by reducing your comp	uter's performance v	here possible.	~
	Show additional plans			
	Change settings that are currently unavail	lable		
	Car .			
See also				
Personalization				
User Accounts				
				~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Start A			B 0	10:34 AM

3. Click High Performance and Change plan settings.

👅 🔵 🗢 🖓 🔹 Control Panel 🔹 A	Control Panel Items + Power Options	- 20	Search Control Panel	
Control Panel Home	Select a power plan			(
Require a password on wakeup	Power plans can help you maximize your computer's po it, or choose a plan and customize it by changing its po			e by selecting
Choose what the power button does	Preferred plans			
Create a power plan	C Balanced (recommended)		Change plan	n settings
Choose when to turn off the display	Automatically balances performance with e	nergy consun	nption on capable hardware.	
	C Power saver		Change plan	n settings
	Saves energy by reducing your computer's p	performance	where possible.	
	Hide additional plans			-
	High performance		Change plan	n settings
	Favors performance, but may use more ene			-

- 4. In the Edit Plan Setting window, click Change settings that are currently unavailable.
- 5. In Turn off the display, select Never, and then click Change advanced power settings.

Edit Plan Settings	in the second second		_ 6 ×
CO V + Al Control Panel Items + Power Options + Edit Plan Settings	- 🖽	Search Control Panel	2
Change settings for the plan: High performance			
Choose the sleep and display settings that you want your computer to	o use.		
😵 Change settings that are currently unavailable			
Turn off the display: 15 minutes			
Change advanced power settings			
😵 Restore default settings for this plan			
	Save	changes Cancel	

6. In the Advanced settings tab of the Power Options window, click Change settings that are currently unavailable. Then click Hard disk > Turn off hard disk after, and select Never.

Power Options		?
Advanced settings		
Select the power plan that you w then choose settings that reflect computer to manage power.	how you want your	
High performance [Active]	•	
🖃 High performance		
Require a password on wakeup Setting: Yes		
🖃 Hard disk		
Turn off hard disk after		
Setting (Minutes): Never	*	
Desktop background settings		
<ul> <li>Wireless Adapter Settings</li> </ul>		
		_
I I USB settings		-
R	estore plan defaults	1
		_
	1	
OK	Cancel Ap	ply

Click Processor power management > Minimum processor state, and then select
 5.

Power Options	<u>-</u>
dvanced settings	
Select the power plan that you want to cus then choose settings that reflect how you computer to manage power.	
High performance [Active]	
Power buttons and lid     PCI Express	<u> </u>
PCI Express     Processor power management	
Minimum processor state	
Setting (%): 5	
System cooling policy	
Maximum processor state	
Display     Multimedia settings	
	-
Restore pla	defaults
	racionits
	1
OK Cancel	Apply

- 8. Click **OK**.
- 9. In the Edit Plan Setting window, click Save change, and then close the window.



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

## **Configuring Action Center settings**

All settings in the Windows Action Center must be disabled.

#### Procedure

 Click Control Panel > Action Center, and then click Change Action Center settings.



2. In the **Change Action Center settings** window, clear all the items, click **OK**, and then close the window.

All Control Panel Items + Action Center + Change	Action Center settings
olt management and	
Turn messages on or off	
For each selected item, Windows will check for p Action Center check for problems?	roblems and send you a message if problems are found. <u>How does</u>
Security messages	
Windows Update	Spyware and related protection
☐ Internet security settings	User Account Control
Network firewall	Virus protection
Maintenance messages	
Windows Backup	Check for updates
Windows Troubleshooting	
Related settings	
Customer Experience Improvement Program	n settings
Problem reporting settings	
Windows Update settings	
	OK Cancel
Note: After configuring Action (	Center settings, configure the
troubleshooting settings.	

### Configuring the troubleshooting settings

The Windows Computer Maintenance setting must be disabled.

#### **Procedure**

1. Click Control Panel > Troubleshooting, and then click Change settings.



2. In the **Change settings** window, for **Computer Maintenance**, click **Off**, and clear all configuration options below **Other settings**.

Change settings	×
CO 🔎 🗷 • All Control Panel Items • Troubleshooting • Change settings	Search Troubleshooting
Change troubleshooting settings	
Computer Maintenance	
Windows will check for routine maintenance issues and remind you when help fix problems. $\bigcirc$ On (Recommended)	n the System Maintenance troubleshooter can
Other settings	
Allow users to browse for troubleshooters available from the Windo	ows Online Troubleshooting service
Allow troubleshooting to begin immediately when started	
Read the privacy statement online	

3. Click **OK**, and then close the window.



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

## **Configuring the Remote Desktop settings**

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

#### Procedure

- 1. Click Control Panel > System, and then click Remote settings.
- 2. In the System Properties window, click the Remote tab.
- **3.** Under **Remote Assistance**, clear **Allow Remote Assistance connections to this computer**.
- 4. Under Remote Desktop, click Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure).

nputer Name   Hardware   Advance	ed System Protection Remote
Remote Assistance	
Allow Remote Assistance conner	ctions to this computer
What happens when I enable Remo	te Assistance?
mist happens when renable mento	
	Advanced
Remote Desktop	
Click an option, and then specify wh	o can connect, if needed.
C Don't allow connections to this c	
Don't allow connections to this c	omputer
Allow connections from compute	rs running any version of
Remote Desktop (less secure)	
<ul> <li>Allow connections only from com Desktop with Network Level Aut</li> </ul>	
Help me choose	Select Users

- 5. Click OK.
- 6. If a message states that the Remote Desktop Firewall will be enabled, click **OK**.

- 7. Click OK to close the System Properties window.
- 8. Close the System window.

-

-

9. Click Control Panel > Windows Firewall, and then click Allow a program or feature through Windows firewall.



10. Click Change settings, and then verify Remote Desktop and Remote Desktop - RemoteFX for both Home/Work (Private) and Public are selected.

llow programs to communicate through Windows Firewall		
add, change, or remove allowed programs and ports, click Change se nat are the risks of allowing a program to communicate?		ge settings
Allowed programs and features:		
Name	Home/Work (Private)	Public 🔺
☑ LPD Service	Ø	
Message Queuing		
Netlogon Service		
Network Discovery		
Performance Logs and Alerts		
Remote Assistance		
Remote Desktop	2	
Remote Desktop - RemoteFX		<b>Z</b>
Remote Event Log Management		
Remote Scheduled Tasks Management		
Remote Service Management		
Remote Volume Management		
Routing and Remote Access		
Secure Socket Tunneling Protocol		
	Details	Remove
	Allow another	program

- **11.** Click **OK**.
- **12.** Close the **Windows Firewall** window.



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

## **Configuring Internet Explorer settings**

Configure Internet Explorer advanced, security, and properties settings.

#### Procedure

1. Click **Control Panel** > **Internet Options**, and then click the **Advanced** tab to modify the settings.

Settings				
G	Accessibility		feelmanne	-
		expand ALT text	or new windows and	tabs
			focus/selection char	herease.
		Confer and the second	m for new windows	
	Reset t	ext size to mediu	m while zooming*	
_	_	oom level for nev	w windows and tabs	
	Browsing			
	and the second second			
	and the second second second		om page layout erro	The Charles and the second second
	Close u	nused folders in H	listory and Favorite	s*
	Close u Disable	nused folders in H	History and Favorite (Internet Explorer)	s*
	Close u Close u Disable Disable Display	nused folders in H script debugging script debugging a notification abo	History and Favorite (Internet Explorer) (Other) out every script error	s*
	Close u Close u Disable Disable Display	nused folders in H script debugging script debugging	History and Favorite (Internet Explorer) (Other) out every script error	s*
•	Close u Disable Disable Display Display	nused folders in H script debugging script debugging a notification abo Accelerator butto	History and Favorite (Internet Explorer) (Other) out every script error on on selection	s*
•	Close u Disable Disable Display Display	nused folders in H script debugging script debugging a notification abo	History and Favorite (Internet Explorer) (Other) out every script error on on selection	s* v L
<b>↓</b> *Tak	Close u Disable Disable Display Display es effect af	nused folders in H script debugging a notification abo Accelerator butto	History and Favorite (Internet Explorer) (Other) out every script error on on selection	s*
*Tak	Close u Disable Disable Display Display es effect af	nused folders in H script debugging a notification abo Accelerator butto fter you restart In forer settings	History and Favorite (Internet Explorer) (Other) out every script error on on selection Internet Explorer Restore ad	s* v L
*Tak Reset Ir	Close u Disable Disable Display Display es effect af	nused folders in H script debugging a notification abo Accelerator butto fter you restart In forer settings	History and Favorite (Internet Explorer) (Other) out every script error on on selection	s* v L
*Tak Reset Ir Reset condi	Close u Disable Disable Display Display s effect af nternet Exp is Internet I tion.	nused folders in H script debugging a notification abo Accelerator butto fter you restart In lorer settings	History and Favorite (Internet Explorer) (Other) out every script error on on selection Internet Explorer Restore ad	r Ivanced settings Reset

2. Under Security, select Allow active content to run in files on My Computer.

ngs				
		results in the ma	ain window	2
Securit		tent from CDs to	run on My (	Computer*
	and the second se	tent to run in file	and the second se	A REAL PROPERTY AND A REAL
		to run or install e		THE PROPERTY AND ADDRESS OF ADDRESS
		her's certificate		
		r certificate revo		221
	March State Reading and	tures on downloa rypted pages to	A REAL PROPERTY OF	ns
		ry Internet Files		browser is do
_	ble DOM Sto			
Ena	DIE DOM Sto			
Ena	ble Integrati	ed Windows Aut		-
	ble Integrat ble native XI	ed Windows Aut MLHTTP support		
	ble Integrati	ed Windows Aut MLHTTP support		
Ena Ena Ena	ble Integrati ble native XI ble SmartScr	ed Windows Aut MLHTTP support reen Filter		
Ena Ena Ena	ble Integrati ble native XI ble SmartScr	ed Windows Aut MLHTTP support	Explorer	Ŀ
Ena Ena Ena akes effe	ble Integrati ble native XI ble SmartScr ct after you i	ed Windows Aut MLHTTP support reen Filter restart Internet	Explorer	vanced setting:
Ena Ena Ena akes effe	ble Integration ble native XI ble SmartScr ct after you i Explorer set	ed Windows Aut MLHTTP support reen Filter restart Internet	Explorer Restore adv	Ŀ
Ena Ena Ena akes effe t Internet sets Inter	ble Integration ble native XI ble SmartScr ct after you i Explorer set	ed Windows Aut MLHTTP support reen Filter restart Internet	Explorer Restore adv	Ŀ
Ena Ena Ena akes effe t Internet sets Internet	ible Integration ible native XI ible SmartSor ct after you i Explorer set net Explorer	ed Windows Aut MLHTTP support reen Filter restart Internet	Explorer Restore ad	vanced settings Reset

- 3. Clear Use SSL 3.0.
- 4. If SSL 2.0 is selected, clear it.
- 5. Select Use TLS 1.0, Use TLS 1.1, and Use TLS 1.2.

	et Proper	ties				1
neral	Security	Privacy Co	ntent   Conr	nections   Pr	ograms	Advance
otting						
etting	5					
	-	Temporary In		folder when	browser	is dc 🔺
		DOM Storage				
		Integrated W				
	and the second second	native XMLH				
	Use St	SmartScreen	Filter			
	Use Ti					
	Use Ti					
	Use Ti	S 1.2				
	V Use T	S 1.2 about certifica	ate address r	nismatch*		
	Varn Warn				cure mod	ie
	Warn Warn	about certifica	tween secur	e and not se		
	Warn Warn	about certifica if changing be	tween secur	e and not se		
•	Warn Warn Warn	about certifica if changing be if POST submit	tween secur ttal is redired	e and not se ted to a zon		
• *Ta	Warn Warn Warn	about certifica if changing be	tween secur ttal is redired	e and not se ted to a zon		
∗Ta	Warn Warn Warn	about certifica if changing be if POST submit	tween secur ttal is redired	e and not se ted to a zon	e that do	es not pe
	Warn Warn Warn	about certifica if changing be if POST submit	tween secur ttal is redired art Internet	e and not se ted to a zon Explorer	e that do	es not pe
eset I	Warn Warn Warn Warn	about certifica if changing be if POST submit after you resta	tween secur ttal is redired art Internet	e and not se ted to a zon Explorer Restore ad	e that do vanced se	ettings
eset I Rese	Warn Warn Warn Warn	about certifica if changing be if POST submit	tween secur ttal is redired art Internet	e and not se ted to a zon Explorer Restore ad	e that do	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect a internet Ex internet Ex ition.	about certifica if changing be if POST submit after you rest plorer settings Explorer's se	tween secur ttal is redired art Internet	e and not se ted to a zon Explorer Restore add	e that do vanced so Rese	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect a internet Ex internet Ex ition.	about certifica if changing be if POST submit after you resta	tween secur ttal is redired art Internet	e and not se ted to a zon Explorer Restore add	e that do vanced so Rese	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect a internet Ex internet Ex ition.	about certifica if changing be if POST submit after you rest plorer settings Explorer's se	tween secur ttal is redired art Internet	e and not se ted to a zon Explorer Restore add	e that do vanced so Rese	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect a internet Ex internet Ex ition.	about certifica if changing be if POST submit after you rest plorer settings Explorer's se	tween secur ttal is redired art Internet	e and not se ted to a zon Explorer Restore add	e that do vanced so Rese	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect a internet Ex internet Ex ition.	about certifica if changing be if POST submit after you rest plorer settings Explorer's se	tween secur ttal is redired art Internet	e and not se ted to a zon Explorer Restore add	e that do vanced so Rese ble state	ettings

- 6. Click **OK**.
- 7. Close the Internet Properties window.
- 8. From the Control Panel window, click System and Security > Action Center.

🕎 Control Panel				- 🗆 ×
GOV - Control Panel •			✓ G Search Control Panel	2
Adjust you	r computer's settings		View by: Category 🕶	
	System and Security Review your computer's status Backu your computer Find and fite problems Network and Internet Verw retwork status and tasls Choose homegroup and sharing options Choose homegroup and sharing options Choose homegroup and sharing options Choose homegroup and sharing options Choose homegroup and sharing options Were devices and printers Add a device Programs Uninstall a program	28. *** ©	User Accounts and Family Safety Set up parental controls for any user Appearance and Personalization Change the theme Change desites badryound Adjust screen resolution Clock, Language, and Region Change keyboards or other input methods Ease of Acces Let Windows suggest settings Optimize visual display	

9. If the SmartScreen Filter window appears, click OK.

	Website addresses will be sent to Microsoft to be checked against a list of reported unsafe websites. Information received will not be used to personally identify you. For more information, read the <u>Internet Explorer privacy statement</u> .	
	OK Cancel	
How	v does SmartScreen Filter help protect me?	

- **10.** Click **All Programs > Internet Explorer**.
- **11.** If the **Set Up Windows Internet Explorer 8** window appears, click **Next**.
- **12.** In the **Turn on Suggested Sites** window, click **No, don't turn on**, and then click **Next**.

Set Up Windows Internet Explorer 8	×
Turn on Suggested Sites	
Do you want to discover websites you might like based on websites you've visited?	
<ul> <li>Yes, turn on Suggested Sites</li> <li>No, don't turn on</li> </ul>	
Suggested Sites is an online service that uses your browsing history to make personalized website suggestions. You can turn off Suggested Sites at any time.	
Read the Internet Explorer Privacy Statement online Back Next Canc	el

**13.** In the **Choose your settings** window, click **Use express settings**, and then click **Finish**.

Set Up Windows Internet Explorer 8	×
Choose your settings	
Before you get started, do you want to:	
<ul> <li>Use express settings Search provider: Bing Search Updates: Download provider updates Accelerators: Blog with Windows Live, Map with Bing, E-mail with Windows Live, Translate with Bing SmartScreen Filter: Enabled Compatibility View: Use updates</li> </ul>	
Choose custom settings Review and modify each setting individually.	
Read the Internet Explorer Privacy Statement online Back Einish Cancel	

**14.** When an error indicates that an Internet connection is not established, close Internet Explorer.



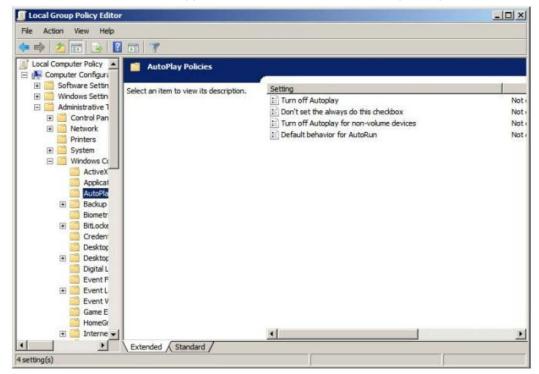
**Note:** After configuring Internet Explorer settings, disable the autoexecute feature.

## Disabling the auto-execute feature

The SVP requires the Windows AutoPlay feature be turned off.

#### Procedure

1. Click Start > Run, and then type gpedit.msc to start the Group Policy Editor.



- 2. Click Local Computer Policy > Computer Configuration, click Administrative Templates > Windows Components, and then click AutoPlay Policies.
- **3.** From the items on the right, double-click **Turn off Autoplay**.

💶 Turn off Autoplay		
Turn off Autoplay	1	Previous Setting
• Not Configured	Comment	3
C Enabled		
C Disabled		<u>×</u>
	Supported on:	At least Windows 2000
Options:		Help:
Turn off Autoplay on	:	Turns off the Autoplay feature.         Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately.         Prior to XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.         Starting with XP SP2, Autoplay is enabled for removable drives as well, including ZIP drives and some USB Mass Storage devices.         If you enable this setting, you can disable Autoplay on CD-ROM and removable media drives, or disable Autoplay on all drives.         This setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default.
Start 🙆 🚞	0	🚺 🐖 🝓 👘 P 🕷 🕼

4. In the **Property** window, click **Enabled** and select **All drives**, and then click **OK**.

Turn off Autoplay			
Turn off Autoplay	e		Erevious Setting Next Setting
C Not Configured	Comment:		
• Enabled			
C Disabled			
	Supported on:	At least Windows 2000	
Options:		1	Help:
furn off Autoplay on		1	Turns off the Autoplay feature.
All drives			Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately.
			Prior to XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.
			Starting with XP SP2, Autoplay is enabled for removable drives as well, including ZIP drives and some USB Mass Storage devices.
			If you enable this setting, you can disable Autoplay on CD-ROM and removable media drives, or disable Autoplay on all drives.
			This setting disables Autoplay on additional types of drives. You cannot use

**5.** Close the Group Policy Editor.

- 6. Click Control Panel > Autoplay.
- 7. Clear Use Autoplay for all media and devices, and then click Save.



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

## **Configuring the Registry**

Use Regedit to edit the Windows Registry on the SVP.

#### Procedure

- 1. Disable anonymous logon (null connection):
  - a. Click **Start** > **Run**, and then type regedit and press **Enter**.

💣 Registry Editor				
File Edit View Favorites Help				
Computer	Name	Туре	Data	
Computer				

- b. In the **User Account Control** menu, click **Yes** to open the **Registry Editor** window.
- c. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control \Lsa.

File Edit View F	avorit				
		FileSystemU 🔺	Name	Туре	Data
	÷	FontAssoc	ab (Default)	REG_SZ	(value not set)
	Ē	GraphicsDriv	auditbasedirectories	REG_DWORD	0x00000000 (0)
	-	GroupOrderi	300 auditbaseobjects	REG_DWORD	0x00000000 (0)
	Ē	HAL	ab Authentication Packa	REG_MULTI_SZ	msv1_0
		hivelist	Bounds	REG_BINARY	00 30 00 00 00 20
	<b>+</b>	IDConfigDB	200 crashonauditfail	REG DWORD	0x00000000 (0)
	<b>H</b>	Keyboard La	100 disabledomaincreds	REG DWORD	0x00000000 (0)
	<b>+</b>	Keyboard La	everyoneincludesano	REG DWORD	0x00000000 (0)
	<b>+</b>	Lsa	forceguest	REG_DWORD	0x00000000 (0)
	<b>.</b>	LsaExtension	100 fullprivilegeauditing	REG BINARY	00
	÷	MediaCateg	100 LimitBlankPasswordUse	REG DWORD	0x00000001 (1)
	+	MediaDRM	100 LsaPid	REG DWORD	0x000001f8 (504)
	÷	MediaInterf	100 NoLmHash	REG DWORD	0x00000001(1)
	÷.	MediaProper	ab Notification Packages	REG MULTI SZ	scecli
		MediaTypes	ProductType	REG_DWORD	0x00000006 (6) _
	<b>H</b> -1	MobilePC	restrictanonymous	REG DWORD	0x00000000 (0)
		MPDEV	100 restrictanonymoussam	REG DWORD	0x00000001 (1)
	<u>h.</u>	MODTO Z		DEG DWODD I	0.00000001(1)
4					<u>)</u>

d. Double-click restrictanonymous.

		Name	Туре	Data
	Edit DWORD (32-bit) Valu Value name: restrictanonymous Value data:	Base	ORD ORD LTI_SZ ARY ORD	(value not set) 0x00000000 (0) 0x00000000 (0) msv1_0 00 30 00 00 00 20 0x00000000 (0)
	1	Hexadecimal     Decimal     OK     Car	ncel ORD	0x00000000 (0) 0x00000000 (0) 0x00000000 (0) 00 0x00000000 (1)
41	MediaDRM     MediaInterfa     MediaProper     MediaTypes     MobilePC     MPDEV     MSDTC	NoLmHash Notification Packages ProductType restrictanonymous	REG_DWORD REG_DWORD REG_MULTI_SZ REG_DWORD REG_DWORD REG_DWORD	0x000001f8 (504) 0x00000001 (1) scecli 0x00000006 (6) 0x00000000 (0) 0x00000000 (1)

- e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.
- 2. Disable the beep when Remote Desktop Connection is connected:
  - a. In the **Registry Editor** window, navigate to HKEY_LOCAL_MACHINE\System \CurrentControlSet\Control\Terminal Server.
  - b. In the **Edit** menu, click **New** > **DWORD** (32-bit) Value.
  - c. Type DisableBeep.

	Session Man	Name	Туре	Data
		(Default)	REG SZ	(value not set)
	SQMServicel	AllowRemoteRPC	REG DWORD	0x00000000 (0)
÷	- Srp	100 DelayConMgrTimeout	REG DWORD	0x00000000 (0)
	SrpExtension	BillipeleteTempDirsOnExit	REG DWORD	0x00000001 (1)
Ē	- 📙 StillImage	100 fDenyTSConnections	REG DWORD	0x00000000 (0)
	- 🚽 Storage	100 fSingleSessionPerUser	REG DWORD	0x00000001 (1)
	- SystemInfor	ab InstanceID	REG SZ	15260f9d-f1fb-46b9
Ē		NotificationTimeOut	REG DWORD	0x00000000 (0)
		RerSessionTempDir	REG DWORD	0x00000000 (0)
±		ab ProductVersion	REG SZ	5.1
	TimeZoneInf	ab RCDependentServices	REG MULTI SZ	CertPropSvc Session
		ab SnapshotMonitors	REG SZ	1
		38 StartRCM	REG DWORD	0x00000000 (0)
		10 TSAdvertise	REG DWORD	0x00000000 (0)
		10 TSUserEnabled	REG DWORD	0x00000000 (0)
		DisableBeep	REG DWORD	0x00000000 (0)
· · · · ·				
		-		•

### d. Double-click **DisableBeep**.

	Session Man 🔺	Name	Туре	Data
Edit DWORD (32-bit Value name: DisableBeep Value data: 1	Base	Hexadecimal Decimal	REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_DWORD REG_DWORD	(value not set) 0x00000000 (0) 0x00000000 (0) 0x0000000 (1) 0x00000000 (0) 0x0000000 (1) 15260f9d-f1fb-46b9 0x00000000 (0) 0x00000000 (0)
	usbstor VAN Video wcncsvc Wdf WDI	OK Cancel SnapshotMonitors StartRCM TSAdvertise TSUserEnabled	REG_SZ REG_MULTI_SZ REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD	5.1 CertPropSvc Session 1 0x00000000 (0) 0x00000000 (0) 0x00000000 (0) 0x00000000 (0)
	+		1	•

- e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.
- **3.** Configure Remote Desktop Connection:
  - a. In the **Registry Editor** window, navigate to <code>HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Terminal Services.</code>

SOFTWARE	Name	Туре	Data
Image: Construction of the second	(Default)	REG_SZ	(value not set) 0x00000000 (0)

- b. In the **Edit** menu, click **New** > **DWORD** (32-bit) Value.
- c. Type fPromptForPassword.
- d. Double-click **fPromptForPassword**.
- e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.

Ē.	SOFTWARE	Name	Туре	Data
	ATT Technolonies     Edit DWORD (32-bit) Value     Value name:     IfPromptForPassword     Value data:     Il     Itrols     ental Controls settings.     Windows NT     Windows NT     Windows     Windows	Base Hexadecimal Decimal	ancel	(value not set) 0x00000000 (0)
	📩 🛄 Conic 🚬 💻	1		

- f. In the **Edit** menu, click **New** > **DWORD** (32-bit) Value.
- g. Type SecurityLayer.

SOFTWARE	Name	Туре	Data
Image: Construction of the second	(Default) (Default) FromptForPassword SecurityLayer	REG_SZ REG_DWORD REG_DWORD	(value not set) 0x00000001 (1) 0x00000000 (0)

4. Restart the server.

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

### Enabling ICMP (ping) reply

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

### Procedure

1. Click Control Panel > Administrative Tools, and then start Windows Firewall with Advanced Security.



2. In the left pane, click Inbound Rules.

Windows Firewall with Advanced S	Inbound Rules					Actions	
Cutbound Rules	Name	Group +	Profile	Enabled	Ac +	Indexed Rates	
Connection Security Rules	Core Networking - Internet Group Management Protoc	Core Networking	Al	Yes	Alle	13 New Rule	
Manitoring	Core Networking - IPHTTPS (TCP-In)	Core Networking	Al	Yes	Alk	The second se	
S. Carriero de	Core Networking - IPv6 (IPv6-In)	Core Networking	Al	Yes	Allı	V Filter by Profile	
	Core Networking - Multicast Listener Done (ICMPv6-In)	Core Networking	Al	Yes	Alt	Filter by State	
	Core Networking - Multicast Listener Query (ICMPv6-In)	Core Networking	Al	Yes	Alic		
	Core Networking - Multicast Listener Report (ICMPv6-In)	Core Networking	AB	Yes	Aå	Titter by Group	
	Core Networking - Multicast Listener Report v2 (ICMPv	Core Networking	AB	Yes	Alt	View	
	Core Networking - Neighbor Discovery Advertisement (	Core Networking	AL	Yes	Abc	Contraction -	
	Core Networking - Neighbor Discovery Solicitation (ICM	Core Networking	Al	Yes	Ali	<u>Ci</u> Refresh	
	Core Networking - Packet Too Big (JCMPv6-br)	Core Networking	Al	Yes	Ab	Export List	
	Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	Al	Yes	Abc	Heb	
	Core Networking - Router Advertisement (ICMPvti-In)	Core Networking	Al	Yes	Alk	E nep	
	Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	Al	Yes	Alt		
	Core Networking - Teredo (UDP-In)	Core Networking	AL	Yes	Alic		
	Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	AL	Yes	Alk	1	
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coordi	Domain	No	Alt	1	
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coord	Privat	No	Ali		
	Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coord	Domain	No	Alle	1	
	Distributed Transaction Coordinator (RPC-EPMAP)	Detributed Transaction Coord	Privat	140	Alt	1	
	Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coord	Privat	No	Abr	1	
	Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coordi	Domain	No	Ab	1	
	File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	No	Alt	1	
	File and Printer Sharing (Echo Request - ICHPv4-In)	File and Printer Sharing	Privat	No	Abr	1	
	File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Privat	No	ASt	1	
	File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No	Abi	1	
	File and Printer Sharing (LLMVR-LOP-In)	File and Printer Sharing	Al	No	Alle	1	
	File and Printer Sharing (H8-Datagram-In)	File and Printer Sharing	Doman	No	Alt	1	
	File and Printer Sharing (H8-Datagram-In)	File and Printer Sharing	Privat	No	ABc	1	
	File and Printer Sharing (NE-Name-In)	File and Printer Sharing	Domain	No	Alt	1	
	File and Printer Sharing (H8-Name-In)	File and Printer Sharing	Privat	No	Alt	1	
	File and Printer Sharing (NE-Session-In)	File and Printer Sharing	Privat	No	Alc	1	
	File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No	Alt	1	
	File and Printer Sharing (SME-In)	File and Printer Sharing	Domain	No	Alt -		
	File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No	Alt		

- 3. Click all the following inbound rules, and then right-click and click **Enable Rules**.
  - File and Printer Sharing (Echo Request ICMPv4-In) (Profile=Domain)
  - File and Printer Sharing (Echo Request ICMPv4-In) (Profile=Private)

- File and Printer Sharing (Echo Request ICMPv6-In) (Profile=Domain)
- File and Printer Sharing (Echo Request ICMPv6-In) (Profile=Private)

	Al Al Al Al Al Al Al Al Al	Enabled Yes Yes Yes Yes	Act * Allo Allo Allo	Actions Inbound Roles	
Authornel Rules     Comencton Security Rules     Core Intervorking - Multicast Listemer Done (ICMPV-6-In)     Core Networking     Munitoring     Core Intervorking - Multicast Listemer Report (ICMPV-6-In)     Core Networking     Core Intervorking     Core Inte	****	Yes Yes Yes Yes	Allo Allo	Rendered and the second s	
Connection Security Rules Connection Rules Connection Security Rules Connection Connection Rules Connection Co	* * * *	Yes Yes Yes	Allo	New Rule	
Core Networking - Multicast Listener Report (CMPV-6-In) Core Networking Core Networking - Multicast Listener Report 22 (CMPV-6-In) Core Networking Core Networking - Networking Networking Networking Core Networking - Networking Networking Networking Core Networking - Paradet Too Big (CMPV-6-In) Core Networking Core Networking - Paradet Probem (CMPV-6-In) Core Networking Core Networking - Router Advectment (CMPV-6-In) Core Networking Core Networking - Router Advectment (CMPV-6-In) Core Networking Core Networking - Router Solicitation (CMPV-6-In) Core Networking Core Networking - Time Exceeded (CMPV-6-In) Core Networking Core Networking - Time (COreNet-In) Core Networking Core Networking - Time (CMPV-6-In) Core Networking Core Networking - Time (CMPV-6-In) Core Networking Core Networking - Time (CMPV-6-In) Core Networking Core Networking - Time (SCREMAP) Distributed Transaction Coordinator (NPC) Distributed Transaction Coordinator (NPC) Distributed Transaction Coordinator (CPC-In) Distributed Transaction Coordinator (CPC-In) Distributed Transaction Coordinator (CPC-In) Costributed Transaction Coordinator (CPC-In) Distributed Transaction Coordinator (CPC-In) Distributed Transaction Coordinator (CPC-In) Costributed Transaction Coordinator (CPC-In) Costributed Transaction Coordinator (CPC-In) Distributed Transaction Coordinator (CPC-In) Costributed Trans	43 43 43 43 43	Yesi Yes			
Core Networking - Multicast Lutterer Report v2 (DOPV Core Networking - Neghtbor Dacovery Advertisement Core Networking - Neghtbor Dacovery Advertisement Core Networking - Report Dacovery Advertisement Core Networking - Packet Too Big (DOPVi-6-In) Core Networking - Packet Too Big (DOPVi-6-In) Core Networking - Rauter Solicitation (DC Core Networking - Rauter Solicitation (DOPVi-6-In) Core Networking - Rauter Solicitation (DOPVi-6-In) Core Networking - Rauter Solicitation (DOPVi-6-In) Core Networking - Time Exceeded (DOPVi-6-In) Core Networking - Time Exceeded (DOPVi-6-In) Core Networking - Time Exceeded (DOPVi-6-In) Distributed Transaction Coordinator (NPC) Distributed Transaction Coordinator (NPC) Distributed Transaction Coordinator (NPC) Distributed Transaction Coordinator (NPC - Bittibuted Transaction C Distributed Transaction Coordinator (NPC - Bittibuted Transaction C Pittibuted Transaction C Coordinator (NPC - Bittibuted Transaction C Pittibuted Transaction Coordinator (NPC - Bittibuted Transaction C Pittibuted Transacti	A1 A1	Yes	Allo	V Filter by Profile	
Oran Hetworking - Neighbor Discovery Advertisement Core Hetworking     Oran Hetworking - Neighbor Discovery Sakitation (C Core Hetworking     Oran Hetworking - Reacher Too Big (ICM+v-En)     Oran Hetworking - Parameter Problem (ICM+vEn)     Oran Hetworking - Reacher Solicitation (ICM+vEn)     Oran Hetworking - Terredo (ICM+vEn)     Oran Hetworking     Oranhetworking     Oranhetworkin	A1 A1		122.0	V rater by Prote	
Core Networking - Neighbor Discovery Sakditation (C, Core Networking     Core Networking - Parameter Problem (CVPV-En)     Core Networking     Core Networking - Parameter Problem (CVPV-En)     Core Networking     Core Networking - Parameter Problem (CVPV-En)     Core Networking     Core Networking - Parameter Advectoment (CVPV-En)     Core Networking     Core Networking - Tender 50 (CP-In)     Core Networking     Core Networking - Tender 50 (CP-In)     Core Networking     Core Networking - Tender 50 (CP-In)     Core Networking     Core Networking     Distributed Transaction Coordinator (NPC)     Distributed Transaction Coordinator (NPC-In)     Distributed Transaction Coordinator     Transaction Coordinator     Transaction Coordinator     Transaction Coordinator     Transaction Coordinator     Distributed Transaction Coordinator     Transaction Coordinator     Transaction Coordinator	Al		Allo	Filter by State	
Orer Hetworking - Packet Tos Big (DSP-6-bi)     Core Hetworking     Core Hetworki	A		Allo	Titer by Group	
Core Networking - Parameter Problem (IDNPv6-In) Core Networking Core Networking - Ruster Advertisement (IDNPv6-In) Core Networking Core Networking - Ruster Advertisement (IDNPv6-In) Core Networking Core Networking - Teredo (ILDP-In) Core Networking Core	Al	Yes	Alio		
Core Hetworking - Router Advertisement (ICXPV-5-In)     Core Hetworking     Distributed Transaction Coordinator (RPC)     Distributed Transaction     Coordinator (RPC)     Distributed Transaction     Coordinator (RPC)     Distributed Transaction     Coordinator (RPC)     Distributed Transaction     Coordinator (RPC)     Distributed Transaction     Coordinator (RPC)     Distributed Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     Distributed     Transaction     D		Yes	Allo	Ves	
Core Hetworking - Rauter Solicitation (CxP-v6-In)     Core Hetworking     Core Hetworking - Treedo (LXP-V6-In)     Core Hetworking     Core Hetworking - Treedo (LXP-V6-In)     Core Hetworking     Distributed Transaction Coordinator (RVC)     Distr	Al	Yes	Allo	C Refresh	
Core Networking - Teredo (LOP-In)     Core Networking     Cor	AB	Yes	Allo		
Core Networking - Time Exceeded (IC/PP-6-In)     Core Networking     Distributed Transaction Coordinator (RPC)     Distributed Transaction Coordinator (RPC-BMAP)     File and Printer Sharing     File and Printer Sharing (RPC-BMAP)     File and Printer Sharing     File and Printer Sharing (RPC-BMAP)     File and Printer Sharing     File and Printer Sharing (RPC-BMAP)     File and Printer Sharing     File and Printer Sharing (RPC-BMAP)     File and Printer Sharing     File and Printer Sh	Al	Yes	Alo	Export List	
Distributed Transaction Coordinator (RPC)     Distributed Transaction Coordinator (RPC)     Distributed Transaction Coordinator (RPC, BMAP)     Fie and Pinter Sharing (CHO Request, 100PV-5in)     Fie and Pinter Sharing (CHO Request, 100PV-5in)     Fie and Pinter Sharing (CHO Request, 100PV-5in)     Fie and Pinter Sharing (RPD Repare, 1-100PV-5in)     Fie and Pinter Sharing     Fie and Pinter Sharing (RPD Repare, 1-100PV-5in)     Fie and Pinter Sharing     Fie and Pinter Sharing (RPD Repare, 1-100PV-5in)     Fie and Pinter Sharing     Fie and Pinter Sharing (RPD Repare, 1-10)     Fie and Pinter Sharing     Fie and Pint	AB	Yes	Allo	Heb	
Detributed Transaction Coordinator (RPC)     Detributed Transaction Coordinator (RPC)     Detributed Transaction Coordinator (RPC-EMMP)     Detributed Transaction Coordinator (RPC-EMMP)     Detributed Transaction Coordinator (RPC-EMMP)     Detributed Transaction Coordinator (RPC-MP)     File and Printer Sharing (Edito Reparet - ICMP-4-50)     File and Printer Sharing     File and Printer Sharing (Edito Reparet - ICMP-4-50)     File and Printer Sharing     File and Printer Sharing (Edito Reparet - ICMP-4-50)     File and Printer Sharing	AZ	Yes	Allo	200 A 200 A 200	_
Distributed Transaction Coordinator (RPC-BMAP)     Distributed Transaction Coordinator (RPC-BMAP)     Distributed Transaction Coordinator (RPC-BMAP)     Distributed Transaction Coordinator (RPC-MAP)     Pla and Printer Sharing (Bho Reparet - ICMP-4-bit)     Fla and Printer Sharing (Bho Reparet - ICMP-4-bit)     Fla and Printer Sharing     Distributed Transaction Coordinator (RPC-Bit)     Fla and Printer Sharing     Plae and Printer Sharing (B-Distagram-In)     Fla and Printer Sharing     Plae and Printer Sharing		No	Allo	Selected Items	
Distributed Transaction Coordinator (RPC-EMAM)     Distributed Transaction Coordinator (RPC-EMAM)     Distributed Transaction Coordinator (RPC-HMA)     File and Printer Sharing (Erbit Request - ICMPV-HM)     File and Printer Sharing     File and Printer Sharing (Erbit Request - ICMPV-HM)     File and Printer Sharing     File and Printer Sharing (Erbit Request - ICMPV-HM)     File and Printer Sharing     File	ordi Privat	No	Alio	Disable Rule	_
Distributed Transaction Coordinator (TCP-In)     Distributed Transaction Coordinator (TCP-In)     Distributed Transaction Coordinator (TCP-In)     Distributed Transaction Co     Tel and Printer Sharing (TcP-In)     File and Printer Sharing     Tel a	ordi Domain	No	Allo		
Distributed Transaction Coordinator (TCP-In)     Distributed Transaction C     File and Printer Sharing (Erbo Request - ICRPV-41n)     File and Printer Sharing     File and Printer Sharing (Erbo Request - ICRPV-41n)     File and Printer Sharing     File     File Sharing     File and Printer Sharing     File     File     File And Printer Sharing     File     File     File     File     Fil	ord Privat	. No	Allo	A Cut	
File and Printer Sharing (Echo Request - ICHPV-Fin)     File and Printer Sharing     File and Printer Sharing (Echo Request - ICHPV-Fin)     File and Printer Sharing	ordi Privat	. No	Aão	Copy	
File and Printer Sharing (Scho Request - ICMP+4-b)     File and Printer Sharing     File and Printer Sharing (Erbo Request - ICMP+6-bi)     File and Printer Sharing (Scho Request - ICMP+6-bi)     File and Printer Sharing (IMR-4(D-bi))     File and Printer Sharing     File and Printer Sharing (PE-Datagram-bi)     File and Printer Sharing	ord Domain	No	Aão		
File and Printer Sharing (Edho Request - IORV-6-In)     File and Printer Sharing (Edho Request - IORV-6-In)     File and Printer Sharing (LMRR-IOP-10)     File and Printer Sharing (LMRR-IOP-10)     File and Printer Sharing (B-Oltagram-In)     File and Printer Sharing (B-Oltagram-In)     File and Printer Sharing (B-Oltagram-In)	Domain	Yes	Allo	X Delete	
Rie and Printer Sharing (Echo Request - ICHPv6-In) File and Printer Sharing     (File and Printer Sharing (LVHR-UCP-In) File and Printer Sharing     (File and Printer Sharing (PE-Ostagram-In) File and Printer Sharing     (Pile and Printer Sharing (PE-Ostagram-In) File and Printer Sharing	Privat	. Yes	Ale	Help	
Pile and Proter Sharing (LMR4.4CP-In)     Pile and Proter Sharing     Pile and Proter Sharing (Re-Datagram-In)     Pile and Proter Sharing (Re-Datagram-In)     Pile and Proter Sharing (Re-Datagram-In)	Privat,	- Yes	Alle	El rep	
File and Printer Sharing (18-Datagram-In) File and Printer Sharing File and Printer Sharing (18-Datagram-In) File and Printer Sharing	Domain	Yes	Alle		
Pile and Printer Sharing (HD-Datagram-In) File and Printer Sharing	Al	No	Allo		
	Domain	No	Allo		
	Privat	. No	Allo		
File and Printer Sharing (46-Name-In) File and Printer Sharing	Domain	No	Alle		
File and Printer Sharing (N8-Name-In) File and Printer Sharing	Privat	. No	Aŝo		
File and Printer Sharing (H8-Session-3n) File and Printer Sharing	Privat	. No	Alle		
Pile and Printer Sharing (NB-Session-In) File and Printer Sharing	Domain	No	Allo		
File and Printer Sharing (SMB-In) File and Printer Sharing	Domain	No	Alio		
Pile and Printer Sharing (SMB-In) File and Printer Sharing	Privat	. No	Allo		
File and Printer Sharing (Spooler Service - RPC) File and Printer Sharing	Domain	No	Aão		
File and Printer Sharing (Spooler Service - RPC) File and Printer Sharing	Privat	. No	Alo +	1	

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

### Changing the computer name

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

### Procedure

- 1. Click Control Panel > System, and then click Change settings under Computer name, domain, and workgroup settings.
- 2. In the System Properties window, click the Computer Name tab, and then click Change.

omputer description:	
	For example: "Kitchen Computer" or "Mary's Computer",
ull computer name:	User-PC
Vorkgroup:	WORKGROUP
o use a wizard to join letwork ID.	a domain or workgroup, click Network ID
o rename this comput orkgroup, click Chan	er or change its domain or Change

**3.** In the **Computer Name** field, type SVP-PC.

ompu	an change the name and the membership of this Iter. Changes might affect access to network resources. Information	computer
	.ter name:	Mary's
SVP-F	More Domain:	ork ID
¢	Workgroup: WORKGROUP	inge
	OK Cancel	

**4.** When prompted to restart your computer, click **OK**.

computer. Changes might affect an More information Computer name:			mputer to apply these
SVP-PC	Before resta	rting, save any o	open files and close all programs.
Full computer name: SVP-PC			ок
	More	prk ID	or this Display
Member of			
C Domain:			r restarting this computer)
		inge	a restarting this computery
Workgroup:			
WORKGROUP			
	-11		
	OK Cancel	1	
		-	
	OK Cancel	Apply	1

5. Click Close.

Computer description:		
	For example: "Kitchen Compu Computer".	iter" or "Mary's
full computer name:	SVP-PC	
Vorkgroup:	WORKGROUP	
fo use a wizard to join a Network ID.	a domain or workgroup, click	Network ID
To rename this compute vorkgroup, click Chang	er or change its domain or le.	Change

6. Click Restart Now.

Microsoft Windows		×
You must restart	your computer to apply th	iese changes
Before restarting, say	ve any open files and close all	programs.
	Restart Now	Restart Later

**7.** Wait for the server to restart.

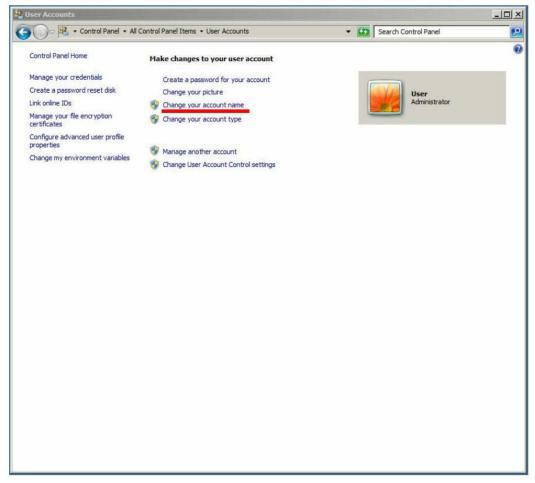
**Note:** After changing the computer name, change the account name.

### Changing the account name

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

#### Procedure

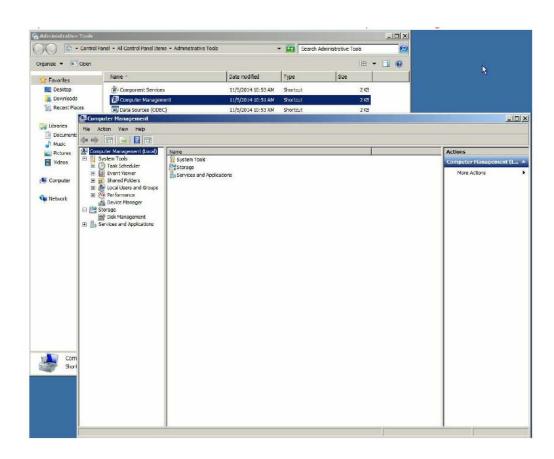
1. Click Control Panel > User Accounts, and then click Change your account name.



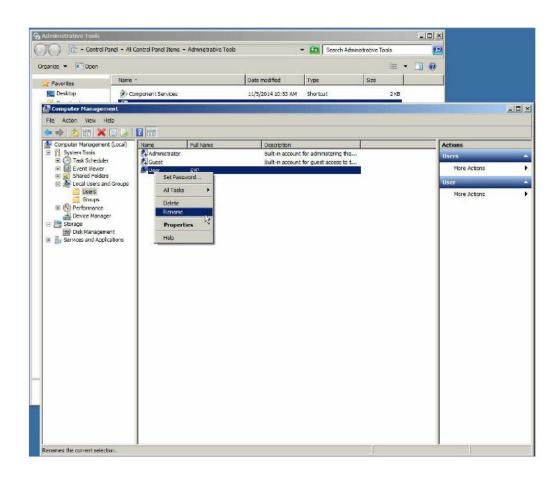
2. Type SVP for the new account name, and then click Change Name.

and the second s	_
Search Co	ntrol Panel
Type a new account name	
User Administrator	
SVP This name will appear on the Welcome screen and on the Start menu.	
Change Name	Cancel

- 3. Close the User Accounts window.
- 4. Click Control Panel > Administrative Tools, and then click Computer Management.



- 5. Click Computer Management (Local) > System Tools, and then click Local Users and Groups > Users.
- 6. In the right window, right-click **User**, and then click **Rename**.



7. Rename User to SVP.

	ol Panel \star All Control Panel	Contractive 10	2	<ul> <li>Search /</li> </ul>	dinado en	
ganize 💌 💽 Open			Date modified	1-	i⊞ ▼ [	11 10 I
Z Favorites	Nome *			Туре	1000	
10 m i i	Component Ser	vices	11/5/2014 10:53 AM	Shortcut	2KB	
Computer Manag						
File Action View	Help 🕇 🗄 📑 🚺 🛅					
Computer Manager		Full Name	Description		1	Actions
E System Tools	Adminis Adminis		Built-in account	t for administering t		Users
🗉 🕐 Task Sched	er SVP	SVP	Built-in account	t for guest access to	1 t	More Actions
E 👔 Shared Fol	ders ders				15	User
Users						More Actions
📄 Groupe 🔃 🕀						
A Device Mar						
E 🔄 Storage	ement					
🗉 🔓 Services and A	oplications					

8. Close the **Computer Management** window, and then close the **Administrative Tools** window.



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

### Configuring the password setting for Administrator

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

### Procedure

1. Click Control Panel > Administrative Tools, and then click Computer Management.

Administrative	Took					_10	×	
00 .	Control Panel - All Control Panel Item	s - Administrative Tools		🕶 🚮 🛛 Search A	Administrative Too	ols		
Organize •	Open					HE + 🔟 🌘	2	10
😤 Favorites	Name +	1	Date modified	Туре	Size			k
E Desktop	A- Component Service		11/5/2014 10:53 AM	Shortcut		2 KB		
😹 Downloads	🔁 Computer Managem	ent	11/5/2014 10:51 AM	Shortnut		2 KB		
🔛 Recent Plac	Cheere see ces less.	.)	11/5/2014 10:53 AM	Shortcut		2.158		
-	Computer Management							
Cibraries	File Action View Help							
Music								
Pictures	Computer Management (Local)	Name						Actions
Videos	E 🔀 System Tools E 🕑 Task Scheduler	System Tools						Computer Management (L., 🔺
-	🗉 🔝 Event Viewer	Services and Application	6					More Actions
🖳 Computer	E and Shared Folders E and Groups							
Network	E 🚳 Performance							
6-	Device Manager							
	Disk Management							
	E Services and Applications							
Com								
Short Short								
						1		

- 2. Click Computer Management (Local) > System Tools, and then click Local Users and Groups > Users.
- **3.** In the right window, right-click **Administrator**, and then click **Set Password**.
- 4. In the warning message, click **Proceed**.

Set Pase	sword for Administrator	×						
	Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user's password is reset.							
	This data loss will occur the next time the user logs off.							
	You should use this command only if a user has forgotten his or her password and does not have a password reset disk. If this user has created a password reset disk, then he or she should use that disk to set the password.							
	If the user knows the password and wants to change it, he or she should log in, then press CTRL+ALT+DELETE and click Change Password.							
	For additional information, click Help.							
	Proceed Cancel Help							

- 5. In the **New password** and **Confirm password** fields, type the administrator password raid-login.
- 6. Click **OK**.

New password:	•••••	
Local	Users and Groups	×
Confirm pass ff you cl This use files, stc	The password has been set.	encrypted
f you click C	ОК	ata loss wil

- 7. Close the **Computer Management** window, and then close the **Administrative Tools** window.
- 8. Restart Windows.

Ē

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

### Changing the password setting

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

### Procedure

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

Create Your Password			
🗸 🗣 🖳 🔹 All Control Panel Items 🔹 User Accounts 🔹 Create Your Password	- 2	Search Control Panel	
Create a password for your account			
SVP Administrator			
••••••			
If your password contains capital letters, they must be typed the same way How to create a strong password	every time y	ou log on.	
Type a password hint			
The password hint will be visible to everyone who uses this computer. What is a password hint?			
	Creat	e password Cancel	

- 4. Click Create password.
- 5. Close the window.

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

## **Configuring Internet Information Services**

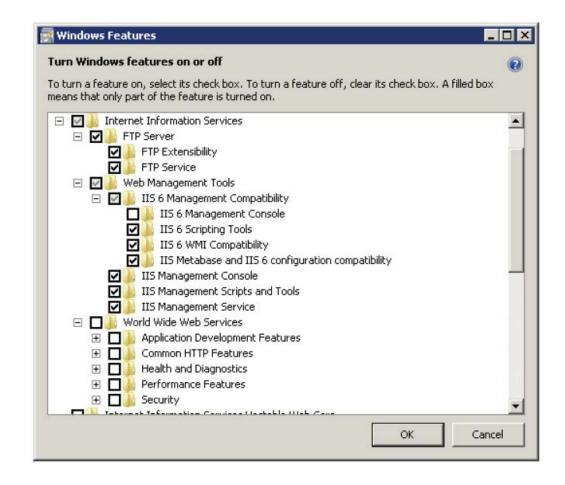
Internet Information Services (IIS) is an extensible web server created by Microsoft for use with Windows operating systems.

### Procedure

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

📰 Windows Features	
Turn Windows features on or off	0
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.	
<ul> <li>Internet Information Services</li> <li>FTP Server</li> <li>FTP Service</li> <li>FTP Service</li> <li>Web Management Tools</li> <li>IIS 6 Management Compatibility</li> <li>IIS 6 Management Console</li> <li>IIS 6 Scripting Tools</li> <li>IIS 6 WMI Compatibility</li> <li>IIS 6 WMI Compatibility</li> <li>IIS Management Console</li> <li>IIS Management Scripts and Tools</li> <li>IIS Management Service</li> <li>World Wide Web Services</li> <li>Application Development Features</li> <li>Common HTTP Features</li> <li>Health and Diagnostics</li> <li>Performance Features</li> <li>Security</li> </ul>	
OK Cance	

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



### Next steps

Install the SVP software.

## Installing the SVP software

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

### Procedure

- **1.** Obtain the appropriate SVP ISO image for your storage system from the firmware distribution set. Verify the ISO image corresponds to the firmware currently running on the storage system.
- **2.** Download the SVP ISO from TISC to the CE notebook, and then use an ISO reader to mount the SVP ISO as the next available drive letter.
- 3. Launch Remote Desktop Connection and click the **Show Options** drop-down menu.



4. Click the Local Resources tab, and then click More.

00	Connection
eneral D	isplay Local Resources Programs Experience Advanced
Remote au	udio Configure remote audio settings. Settings
Keyboard	Apply Windows key combinations:
~	Only when using the full screen   Example: ALT+TAB
Local devi	ces and resources
-	Choose the devices and resources that you want to use in your remote session.
	Printers Clipboard
	Mort.

- **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.

Computer 💭							-	. 🗆 >
GO + Computer	*				• 🔛 Search Computer			
Organize 🔻 System proper	ties Uninstall or change a program Ma	p network drive Open Control Panel				11 h	• 🗖	
E 🚖 Favorites E Desktop Downloads E Recent Places	Hard Disk Drives (1)      Local Disk (C:)      78.5 GB free of 99.8 GB      Devices with Removable Storage (2)							
<ul> <li>□ □ Libraries</li> <li>□ □ Documents</li> <li>□ ↓ Music</li> <li>□ □ Pictures</li> <li>① □ Videos</li> </ul>	Floppy Disk Drive (A:)	DVD Drive (D:) 0 bytes free of 0 votescely CDFS	DKCMAIN_SVP_8 1.02 GB	3303				
Computer Coll Disk (C:) Coll Disk (C:) Coll Disk (D:) DKCMA Coll Disk (D:) DKCMA Coll Disk (D:) DKCMA								
🗄 📬 Network								
	kgroup: WORKGROUP Memo ccessor: Intel(R) Xeon(R) CPU E5	ry: 8.00 GB						_
E on USSCC-RMEJIA2								
😋 🔾 🖓 🗣 🔹 Computer	✓ E on USSCC-RMEJIA2				👻 🔛 🛛 Search E on USSC	C-RMEJIA2		
Organize 🔻						38	• 🔟	
🖂 🚖 Favorites	Name *	Date modified	Туре	Size				
E Desktop	📕 firmware	1/13/2016 11:22 PM	File folder					
Downloads	鷆 oss	1/13/2016 11:22 PM	File folder					
🔛 Recent Places	RaidManager	1/13/2016 11:22 PM	File folder					
and the second second second	Setup2K	1/13/2016 11:22 PM	File folder					
E 🔚 Libraries	Software	1/13/2016 11:22 PM	File folder					
	tool	1/13/2016 11:22 PM	File folder					
E Pictures	Setup	1/13/2016 11:08 AM	Application	60 KB				
E Videos	$\smile$							
E 📑 <u>Computer</u> E 💒 Lo&Disk (C:)								
DVD Drive (D:) DKCMA     E on USSCC-RMEJIA2								
🗄 📬 Network								
7 items								_

- 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.

			Hitachi Devi	e Manager - Storage Navigator		- 🗆 X
Environme	ntal Settir	igs			0	HITACHI
Discontinued				e of the storage system.		
			firmware or the softwar	e of the storage system.		_
SVP IP Address:	IPv4	O IPv6		Г		
				_		
					Apply	Cancel

- 11. Click Apply.
- **12.** Add the storage system.

🐅 Hitachi Device Manager - Storage Navigator			_ 🗆 ×
Environmental Settings			HITACHI
In the case of adding the storage system, push [Add] button. In the case of changing the target of update, select the storage In the case of editing the setting of the storage system, select th	systems and push [Selec he storage system and p	st Update Objects] button. ush [Edit] button. Push [Apply] button for executing setup.	
	Add System Set values for the new	System and click [Apply] to confirm.	Refresh
Storage Systems			
Select All	System Selection:	Auto Discovery	
System Name Type	IP Address (CTL1):	● IPv4 ○ IPv6	sion (Storage System)
	IP Address (CTL2):	IPv4  IPv6	
	System Name:	VSP 6800 (Max, 180 characters)	
	Description:	VSP 6800	
		(Max, 180 characters, or blank)	
	User Name:	maintenance (Max, 256 characters)	
	Password:		
Add Select Update Objects Edit	Not start service a	fter addition immediately	Selected: 0 of 0
Concercitivate orderite		Apply Cancel	
			Apply Cancel

**13.** Register the storage system.

	I Settings			нп/
he case of changing	e storage system, push [Add] button the target of update, select the stora	age systems and push [Sel	ect Update Objects] button. push [Edit] button. Push [Apply] button for executing	
re case or editing th	e seung or me storage system, sele	or the storage system and	posit (car) outon. Fosit (Apply) outon for executin	g serup.
				Refresh
Storage Syst	ame			
Select All	ema			
System Name	Туре	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
VSPG800	VSP 0800 and VSP F800	XXXXXXXXX	-> 83-03-02-60/00	83-03-01-60/00 -> 83-03-02-60/00
Add	ect Update Objects	Remove		Selected: 0 of 1

**14.** Click the storage system.

You are presented with the following two options:

- Upgrading the firmware and adding the storage system
- Adding the storage system without upgrading the firmware
- **15.** If the storage system firmware is current, click **Select Update Objects** and clear **Firmware (Storage System)**. Doing so adds the storage system without upgrading the firmware.

Storage Syst	ame					Refresh
Select All						
System Name	Ty VSP 6800 and VSP	pe Select Update D	Serial Number	Software Version (Storage Navigator)	Firmware Version (Stora 60/00 -> 83-03-02-60/00	ige System)
			Firmwate	e (Storage System)		

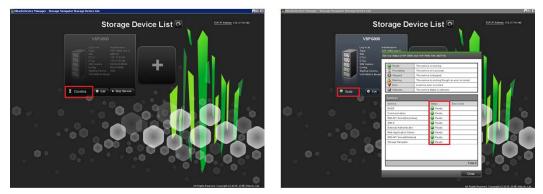
**16.** Click **Apply**, and then click **Confirm** to added the storage system to the SVP.

	al Settings			0///	HITA
e software update in sh [Update] button fo software and firmw	progress. r starting the firmware update. are are updated, push [Close] button	for exit the Environmenta	I Settings.		
System Name	Туре	Serial Number	Software (Storage Navigator)	Firmwa	are (Storage System)
VSP6800	VSP G800 and VSP F800	XXXXXXXX	🕑 Completed	(Not Update)	Update
				_	

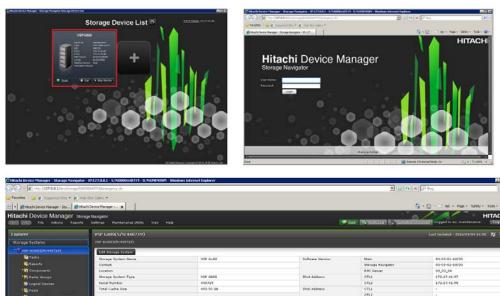
**17.** On the Desktop, click the **Open StorageDevice List** shortcut.



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



**18.** 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

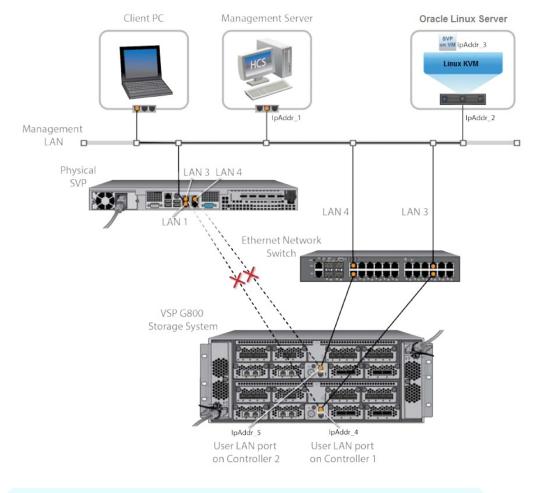
Hitachi Vantara supports configurations where a single SVP communicates with a single VSP Gx00 or VSP Fx00 model. This configuration can coexist with, or replace, all other physical, virtual, and bare-metal SVP configurations.

## 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 KVMbased SVP configuration using the Hitachi Virtual Storage Platform G800. Adjust your connections appropriately if you use different VSP Gx00 models or VSP Fx00 models.

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



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

If the controllers are connected to a physical SVP, remove the Ethernet cables from the LAN3 and LAN4 ports on the SVP, and connect them to the network switch.

## Minimum requirements for an Oracle Linux KVM SVP

An SVP that will be used in an Oracle Linux KVM environment requires the following minimum requirements.

### Prerequisites

Linux KVM Server (provided by the customer)

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

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

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

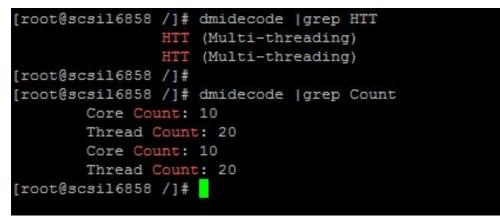
### Miscellaneous

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.



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

		virtual	SVP_1	/irtual	Machi	ne		- ×
File Virtual Machine View	Send Key							
	• 6							•
🖳 Overview	CPUs							
Performance	Logical ho	st CPUs	: 20					
Processor	Current a	llocation	2	-	+			
🚟 Memory				-	E.			
Boot Options	Maximum a	llocation	: 4		+			
IDE Disk 1	Configuratio	n						
🚅 NIC :15:c0:c7	Copy ho	st CPU o	onfigura	tion				
👌 Mouse	Model: H	aswell-n	oTSX		•			
🛋 Keyboard								
🛒 Display Spice	▼ Topology							
텔 Sound: ich6	🗹 Manua	illy set C	PU topo	logy				
🚵 Serial 1	Sockets:	2	- +					
Channel spice	Cores:	1	- +	1				
🖳 Video QXL				i				
Controller USB	Threads:	2	- +	J				
Controller PCI	▼ Pinning							
Controller IDE	Default pir	nning:				(ex: 0, 1, 3 - 5, 7)		
Controller VirtIO Serial		Ē						
😲 USB Redirector 1			Generat	e from	host N	IUMA configuration		
USB Redirector 2								
Add Hardware							Cancel	Apply

## 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.

		QEMU/KVM Co	nnection Details	-	•	
e						
Overview	Virtual Networks	Storage	Network Interfaces			
br0	Bridge brO	:				
ens255f0	MAC:	Unknown				
ens9	State:	⊵ Active				
lo	Start mode	onboot 💌				
	In use hur	-				
	In use by:					
		nfiguration				
		tatic				
	Address: 1	72.17.68.58/24				
	► IPv6 Co	nfiguration				
	Slave Inter	faces				
	Name 🔻	Interface Type				
	ens255f1	ethernet				
	vnet0	ethernet				
	vnet1	ethernet				
	vnet2	ethernet				
	vnet3	ethernet				
+ 🕨 🐰 (	8				App	p

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

net Protocol Version 4 (TCP/I	PV4) Prop	bert	es	_		
neral						
ou can get IP settings assigned aut is capability. Otherwise, you need r the appropriate IP settings.						
C Obtain an IP address automatic	cally					
Use the following IP address: –						_
IP address:			•	÷		
Subnet mask:	255 .	255	. 255		0	
Default gateway:				•		
C Obtain DN5 server address aut	omatically					
• Use the following DNS server a	ddresses:					
Preferred DNS server:		_				
Alternate DNS server:				÷		
Validate settings upon exit				A	dvanced	
				_		nc

**4.** Configure a Remote Desktop connection.

tem Properties			
omputer Name   Hardware	Advanced	System Protection	Remote
Remote Assistance			
Allow Remote Assistar	nce connections	s to this computer	
What happens when I end	able Remote As	sistance?	
		Ad	vanced
Remote Desktop			
Click an option, and then	specify who car	n connect, if neede	d.
C Don't allow connection	ns to this compu	iter	
C Allow connections from Remote Desktop (less		ning any version o	f
<ul> <li>Allow connections only Desktop with Network</li> </ul>			9)
Help me choose		Sele	ect Users
	OK	Cancel	Apply

## Where to go from here

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

### Procedure

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

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

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

Observe the following guidelines when installing a virtual SVP:

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

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

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

### Setting up the SVP locale

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

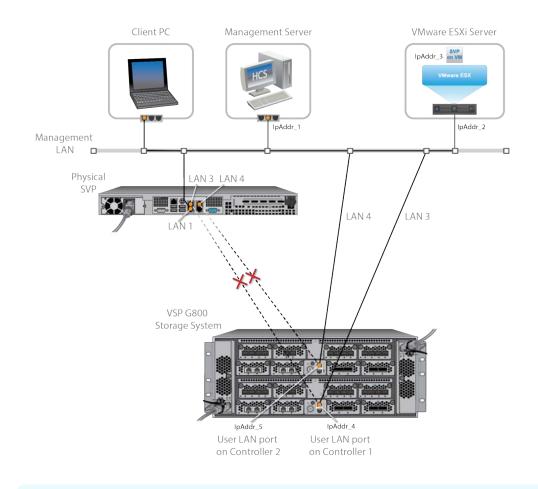
If you intend to install the SVP software using a language other than English and Japanese, change the SVP's locale setting to reflect the appropriate language using the procedure for the Windows version installed on the SVP. For more information, see the instructions for your Windows operating system.

## Network connection for virtual SVP

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

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

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



**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

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

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

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

#### Miscellaneous

WinZip

# Hyper-threading

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



**Note:** Hyper-threading is enabled by default.

<u>ESXi</u> server		VM gues	st host	
2.17.74.130 VHware ESXi, 6.0.0, 3029758		0	scsilvm74140_SVP_WI	ES7 - Virtual Machine Properties
Getting Started Summary Virtu	al Machines Resource Allocation	Hardware Options Resour	ces vServices	Virtual Machine Version: 11 🧕
General		Settings	Summary	
Manufacturer: Model: CPU Cores:	Quanta Computer Inc D518-2U (dual 10G LoM) 20 CPUs x 2.294 GHz	CPU Memory Disk	0 MHz 0 MB Normal	Hyperthreaded Core Sharing Mode: Any Allow sharing of physical CPU cores when the host supports hyperthreading.
Processor Type:	Intel(R) Xeon(R) CPU ES-2650 v3 @ 2,30GHz	Advanced CPU Advanced Memory	HT Sharing: Any NUMA Nodes: 2	nypertrireading.
License: Processor Sockets: Cores per Socket: Logical Processors:	VMware vSphere 6 Enterprise Plus - Licensed for 2 physic 2 10 40	Auvaliceu Helikiy	NUMA NUUB. 2	Schedulino Affinity. Hyperthreading Status: Active Available CPUS: 40 (logical CPUs) Select logical processor affinity for this virtual machine.
Hyperthreading: Number of NiLS:	Active			Use '-' for ranges and ',' to separate values. For example, '0,2-4,7' would indicate processors 0, 2, 3, 4, and 7.
State:	Connected			Clear the string to remove affinity settings.
Virtual Machines and Templates:	15			
vMotion Enabled:	No			
VMware EVC Mode:	Disabled 🖓			
vSphere HA State	③ N/A			
Host Configured for FT:	No 🗘			

# **Configuring the virtual SVP**

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

#### Procedure

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

0		Virtual Machine Properties
Hardware Options Resources vS	ervices	Virtual Machine Version: 11 🛕
Show All Devices	Add Remove	Connected
Hardware	Summary	Connect at power on
Memory (edited)	4096 MB	Adapter Type
CPUs	1	Current adapter: E1000
Video card	Video card	
VMCI device SCSI controller 0	Deprecated	MAC Address
	LSI Logic SAS [datastore1 (4)] H8-SV	
CD/DVD drive 1 Hard disk 1	Virtual Disk	Automatic C Manual
Floppy drive 1	Client Device	
Network adapter 1	VM Network	DirectPath I/O
		Status: Not supported 🕕
		Network Connection
		Network label:
		VM Network
		private
		VM Network
<u>/</u>		
		OK Cancel

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

sk yo	our ne		admir ,	support histrator
255			. 0	
255			. 0	
255			. 0	
255	. 255	. 255	. 0	_
	•	•		
tical	V			
	50.			
_				
_		•		
			Adv	anced
		·	esses:	esses: • • • • • • Adv

**4.** Configure a Remote Desktop connection.

tem Properties			
omputer Name   Hardv	vare Advanced	System Protection	Remote
Remote Assistance			
Allow Remote Ass	sistance connection	s to this computer	
What happens when	I enable Remote As	ssistance?	
		Ad	vanced
Remote Desktop			
Click an option, and t	hen specify who ca	n connect, if neede	d.
C Don't allow conne	ections to this comp	uter	
C Allow connections Remote Desktop		nning any version o	f
<ul> <li>Allow connections Desktop with Net</li> </ul>	s only from compute work Level Authent		e)
Help me choose		Sele	ect Users



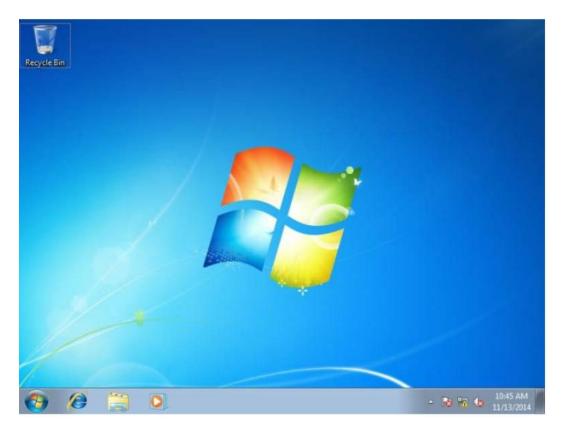
**Note:** After completing the configuration task, configure the SVP guest OS.

# Configuring the SVP guest OS

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

## Logging on to the operating system

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



After logging on successfully, configure the control panel display.

## **Configuring the Control Panel display**

### Procedure

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

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

## **Configuring the desktop**

Configure the Windows screen saver function on the SVP.

### Procedure

1. Click Control Panel > Personalization. For Basic and High Contrast Themes (6), click Windows Classic.



- 2. Click Screen saver.
- 3. In Screen saver, click Blank, and then set Wait to 60 (minutes).
- 4. Click **OK**.

and the second h			
reen Saver			
		.0	
Screen saver		1	
Screen saver	<b>_</b>	Settings	Preview
Blank	<b>.</b>		
Blank	▼ inutes 「 On resur		
Blank Wait: 60 🛨 m	▼ inutes 「 On resur		
Blank Wait: 60 🛨 m Power management		me, display logon	screen
Blank Wait: 60 🛨 m	naximize performa	me, display logon	screen
Blank Wait: 60 1 m Power management Conserve energy or r brightness and other	naximize performa power settings.	me, display logon	screen
Blank Wait: 60 🛨 m Power management Conserve energy or r	naximize performa power settings.	me, display logon	screen
Blank Wait: 60 1 m Power management Conserve energy or r brightness and other	naximize performa power settings.	me, display logon	screen

### Next steps

Configure the task bar and the start menu properties.

## Configuring the task bar and the start menu properties

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

### Procedure

- 1. Click Control Panel > Taskbar and Start Menu Properties (task bar property), and then click the Taskbar tab.
- 2. Click Customize.

Taskbar appearance         ✓ Lock the taskbar         ✓ Auto-hide the taskbar         ✓ Use small icons         Taskbar location on screen:         Bottom         Taskbar buttons:         Always combine, hide labels         Notification area	_
Use small icons Taskbar location on screen: Bottom Taskbar buttons: Always combine, hide labels	_
Taskbar location on screen:     Bottom       Taskbar buttons:     Always combine, hide labels	_
Taskbar buttons: Always combine, hide labels	-
	-
Notification area	-
notification area.	
Preview desktop with Aero Peek	
Temporarily view the desktop when you move your mouse to the Show desktop button at end of the taskbar.	2
Use Aero Peek to preview the desktop	

3. In the Notification Area Icons window, check Always show all icons and notifications on the taskbar.

- Control Panel - All Control Panel Items - Notification	on Area Icons	- 🔛	Search Control Panel	
Select which icons and notifications appear on the If you choose to hide icons and notifications, you won't click the arrow next to the notification area on the tasks	be notified about changes or	updates. To	o view hidden icons at any	time,
Icons	Behaviors			-
Action Center Solve PC issues: 2 important messages	Show icon and not	ifications	÷.	
Network Not Connected You are currently not co	Show icon and not	ifications		
Volume No Audio Output Device is installed.	Show icon and not	ifications	÷	
Windows Explorer Safely Remove Hardware and Eject Me	Only show notifica	tions	Ŧ	_
Windows host process (Rundll32)	Only show notifica	tionș	*	-
Turn system icons on or off				
Restore default icon behaviors				
Always show all icons and notifications on the taskba	ar			

- **4.** Click **OK**.
- 5. Click Control Panel > Taskbar and Start Menu Properties (task bar property), and then click the Start Menu tab.
- 6. Click Customize.

Taskbar Start Menu	Toolbars	
To customize how links behave in the Start me	, icons, and menus look and enu, click Customize.	Customize
Power button action:	Shut down	•
Privacy		
Store and displat	y recently opened programs i	n the Start menu
Store and displating the taskbar	y recently opened items in the	e Start menu and
	way the Start many looks?	
How do I change the v	vay the Start mentionoks?	
How do I change the v	vay ule Startment looks:	

7. In the Customize Start Menu window, check Run command and click Display on the All Programs menu and the Start menu.

O Display as a link	-
O Display as a menu	
<ul> <li>Don't display this item</li> </ul>	
Run command	
Search other files and libraries	
O Don't search	
O Search with public folders	
<ul> <li>Search without public folders</li> </ul>	
Search programs and Control Panel	
Sort All Programs menu by name	
System administrative tools	
O Display on the All Programs menu	
Display on the All Programs menu and the Star	tmenu
O Don't display this item	
Use large icons	
Videos	
O Display as a link	
Start menu size	
Number of recent programs to display:	10 🛨
Number of recent items to display in Jump Lists:	10 +

8. Under Music, check Don't display this item.

	O Display as a menu	10000
-	<ul> <li>Don't display this item</li> </ul>	
⊻	Enable context menus and dragging and dropping	
	Favorites menu	
P	Games	
	O Display as a link	
	O Display as a menu	
_	O Don't display this item	
ビ	Help	-
넫	Highlight newly installed programs	
ų	Homegroup	
d	Music	
	O Display as a link O Display as a menu	
	<ul> <li>Display as a menu</li> <li>Don't display this item</li> </ul>	
п	Network	
님	Open submenus when I pause on them with the mouse pointer	Ĩ.
Ľ	open submenus where pouse on a len war are mouse pointer	1
Sta	art menu size	_
Nu	mber of recent programs to display:	-
Nu	mber of recent items to display in Jump Lists: 10 -	

- 9. Click OK.
- **10.** In the **Taskbar and Start Menu Properties** window, click **OK**.

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

## Configuring the time settings

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

### Procedure

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



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

## **Configuring region settings**

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

### Procedure

1. Click Control Panel > Region and Language, and then click the Keyboards and Languages tab.

mats	Location	Keyboards and	d Languages Administrative
Keybo	oards and	other input la	nguages
To ch	nange you	ir keyboard or	input language click Change keyboards.
			Change keyboards
How	do I chan	ge the keyboa	rd layout for the Welcome screen?
Displa	ay languag	ge	
			s that Windows can use to display text and speech and handwriting.
write	re suppor	ted recognize :	
			Install/uninstall languages
łow c	an I install	l additional lan	i <u>guages?</u>

- 2. Click Change keyboards.
- 3. In the Text Service and Input Languages window, click the Language Bar tab.
- 4. Click Hidden, and then click OK.

Pregion and Language	×
Formats Location Keyboards and Languages Administrative	
Services and Input Languages	×
General Language Bar Advanced Key Settings	
Language Bar C Eloating On Desktop C Docked in the taskbar C Hidden	
<ul> <li>Show the Language bar as transparent when injactive</li> <li>Show additional Language bar icons in the taskbar</li> <li>Show text labels on the Language bar</li> </ul>	
OK Cancel	Apply

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

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



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

## Configuring the power management settings

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

#### Procedure

- Click Control Panel > Power Options, and then click the Show additional plans list.
- 2. Click Change settings that are currently unavailable.

- Control Panel - A	I Control Panel Items + Power Options	- 🖙	Search Control Panel	1
Control Panel Home				6
Control Panel Home	Select a power plan			
Choose what the power button does	Power plans can help you maximize your compu- it, or choose a plan and customize it by changing the second	iter's performance or o ig its power settings. ]	conserve energy. Make a Tell me more about powe	a plan active by selecting <u>er plans</u>
Create a power plan	Preferred plans			
Choose when to turn off the	@ Balanced (recommended)		(	Change plan settings
display	Automatically balances performance	with energy consum	nption on capable har	dware.
	C Power saver		(	Change plan settings
	Saves energy by reducing your comp	uter's performance	where possible.	~
	Show additional plans			
	Change settings that are currently unavail	able		
	R			
See also				
Personalization				
User Accounts				
	-			2012231
Start A			in	10:34 AM

3. Click High Performance and Change plan settings.

👅 🔵 🗢 🖓 🔹 Control Panel 🔹 A	Control Panel Items + Power Options	- 20	Search Control Panel	
Control Panel Home	Select a power plan			(
Require a password on wakeup	Power plans can help you maximize your computer's po it, or choose a plan and customize it by changing its po			e by selecting
Choose what the power button does	Preferred plans			
Create a power plan	C Balanced (recommended)		Change plan	n settings
Choose when to turn off the display	Automatically balances performance with e	nergy consun	nption on capable hardware.	
	C Power saver		Change plan	n settings
	Saves energy by reducing your computer's p	performance	where possible.	
	Hide additional plans			-
	High performance		Change plan	n settings
	Favors performance, but may use more ene			-

- 4. In the Edit Plan Setting window, click Change settings that are currently unavailable.
- 5. In Turn off the display, select Never, and then click Change advanced power settings.

Edit Plan Settings	terre (		_ 6 ×
CO V + Al Control Panel Items + Power Options + Edit Plan Settings	- 🖽	Search Control Panel	2
Change settings for the plan: High performance			
Choose the sleep and display settings that you want your computer to	o use.		
😵 Change settings that are currently unavailable			
Turn off the display: 15 minutes			
Change advanced power settings			
😵 Restore default settings for this plan			
	Save	changes Cancel	

6. In the Advanced settings tab of the Power Options window, click Change settings that are currently unavailable. Then click Hard disk > Turn off hard disk after, and select Never.

Power Options		?
Advanced settings		
Select the power plan that you w then choose settings that reflect computer to manage power.	how you want your	
High performance [Active]	•	
🖃 High performance		
Require a password on wakeup Setting: Yes		
🖃 Hard disk		
Turn off hard disk after		
Setting (Minutes): Never	*	
Desktop background settings		
<ul> <li>Wireless Adapter Settings</li> </ul>		
		_
I I USB settings		-
R	estore plan defaults	1
		_
	1	
OK	Cancel Ap	ply

Click Processor power management > Minimum processor state, and then select
 5.

Power Options	<u>_</u>
dvanced settings	
Select the power plan that you want to cus then choose settings that reflect how you computer to manage power.	
High performance [Active]	
Power buttons and lid     PCI Express	<u> </u>
PCI Express     Processor power management	
Minimum processor state	
Setting (%): 5	
System cooling policy	
Maximum processor state	
Display     Multimedia settings	
	-
Restore pla	defaults
	racionits
	1
OK Cancel	Apply

- 8. Click **OK**.
- 9. In the Edit Plan Setting window, click Save change, and then close the window.

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

## **Configuring Action Center settings**

All settings in the Windows Action Center must be disabled.

#### Procedure

 Click Control Panel > Action Center, and then click Change Action Center settings.



2. In the **Change Action Center settings** window, clear all the items, click **OK**, and then close the window.

All Control Panel Items + Action Center + Change	Action Center settings
oli interne interne ereter	
Turn messages on or off	
For each selected item, Windows will check for p Action Center check for problems?	roblems and send you a message if problems are found. <u>How does</u>
Security messages	
Windows Update	Spyware and related protection
☐ Internet security settings	User Account Control
Network firewall	Virus protection
Maintenance messages	
Windows Backup	Check for updates
Windows Troubleshooting	
Related settings	
Customer Experience Improvement Program	n settings
Problem reporting settings	
Windows Update settings	
	OK Cancel
Note: After configuring Action (	Center settings, configure the
troubleshooting settings.	

### Configuring the troubleshooting settings

The Windows Computer Maintenance setting must be disabled.

#### **Procedure**

1. Click Control Panel > Troubleshooting, and then click Change settings.



2. In the **Change settings** window, for **Computer Maintenance**, click **Off**, and clear all configuration options below **Other settings**.

Change settings			_ 8 ×
COO 📧 • All Control Panel Items • Troubleshooting • Change settings	• (	Search Troubleshooting	2
Change troubleshooting settings			
Computer Maintenance			
Windows will check for routine maintenance issues and remind you when help fix problems. C On (Recommended)	the System Ma	intenance troubleshooter can	
€ off			
Other settings			
Allow users to browse for troubleshooters available from the Window	s Online Troubl	eshooting service	
Allow troubleshooting to begin immediately when started			
Read the privacy statement online			

3. Click **OK**, and then close the window.



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

## **Configuring the Remote Desktop settings**

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

#### Procedure

- 1. Click Control Panel > System, and then click Remote settings.
- 2. In the System Properties window, click the Remote tab.
- **3.** Under **Remote Assistance**, clear **Allow Remote Assistance connections to this computer**.
- 4. Under Remote Desktop, click Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure).

nputer Name   Hardware   Advance	ed System Protection Remote
Remote Assistance	
Allow Remote Assistance conner	ctions to this computer
What happens when I enable Remo	te Assistance?
mist happens when renable mento	
	Advanced
Remote Desktop	
Click an option, and then specify wh	o can connect, if needed.
C Don't allow connections to this c	
Don't allow connections to this c	omputer
Allow connections from compute	rs running any version of
Remote Desktop (less secure)	
<ul> <li>Allow connections only from com Desktop with Network Level Aut</li> </ul>	
Help me choose	Select Users

- 5. Click **OK**.
- 6. If a message states that the Remote Desktop Firewall will be enabled, click **OK**.

- 7. Click OK to close the System Properties window.
- 8. Close the System window.

-

9. Click Control Panel > Windows Firewall, and then click Allow a program or feature through Windows firewall.



10. Click Change settings, and then verify Remote Desktop and Remote Desktop - RemoteFX for both Home/Work (Private) and Public are selected.

low programs to communicate through Windows Firewall		
add, change, or remove allowed programs and ports, click Change set	1011 - 101-	
at are the risks of allowing a program to communicate?	Chan	ge settings
Allowed programs and features:		
Name	Home/Work (Private)	Public 🔺
LPD Service		•
Message Queuing		
Netlogon Service		
Network Discovery		
Performance Logs and Alerts		
Remote Assistance		
Remote Desktop		
Remote Desktop - RemoteFX		2
Remote Event Log Management		
Remote Scheduled Tasks Management		
Remote Service Management		
Remote Volume Management		
Routing and Remote Access		
Secure Socket Tunnelino Protocol		
	Details	Remove
	Allow another	program

- **11.** Click **OK**.
- **12.** Close the **Windows Firewall** window.



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

# **Configuring Internet Explorer settings**

Configure Internet Explorer advanced, security, and properties settings.

### Procedure

1. Click **Control Panel** > **Internet Options**, and then click the **Advanced** tab to modify the settings.

ettings					
G	Accessibili		ut fas ins sea		-
	_	s expand ALT te	for new windows	and tabs	
-			h focus/selection		_
		a second second second second second	ium for new windo		abs
	Reset	text size to med	lium while zooming	*	
-	_	zoom level for n	ew windows and t	abs	
	Browsing				
		- 42 B	C		al an
			from page layout		th Compa
	Close	unused folders in	h History and Favo	rites*	th Compa
	Close	unused folders in	n History and Favo ng (Internet Explo	rites*	th Compa
	Close Close Disable Disable	unused folders ir e script debuggir e script debuggir	n History and Favo ng (Internet Explo	rites* rer)	th Compa
	Close Close Disable Disable Disable Displa	unused folders in a script debuggir a script debuggir a notification a	n History and Favo ng (Internet Explo ng (Other)	rites* rer)	th Compa
•	Close Disable Disable Disable Displa	unused folders in e script debuggir e script debuggir y a notification a y Accelerator bu	n History and Favo ng (Internet Explo ng (Other) bout every script tton on selection	rites* rer) error	th Compa
•	Close Disable Disable Disable Displa	unused folders in e script debuggir e script debuggir y a notification a y Accelerator bu	n History and Favo ng (Internet Explo ng (Other) bout every script tton on selection	error	<u>ب</u>
•	Close Disable Disable Disable Displa	unused folders in e script debuggir e script debuggir y a notification a y Accelerator bu	n History and Favo ng (Internet Explo ng (Other) bout every script tton on selection	error	th Compa
₹ *Tak	Close Disable Disable Displa Displa es effect a	unused folders in e script debuggir e script debuggir y a notification a y Accelerator bu	n History and Favo ng (Internet Explo ng (Other) bout every script tton on selection	error	<u>ب</u>
₹Tak *Tak	Close Disable Disable Displa Displa es effect a nternet Ex	unused folders ir e script debuggir e script debuggir y a notification a y Accelerator bu after you restart	n History and Favo ng (Internet Explo ng (Other) bout every script tton on selection	error	<u>ب</u>
*Tak Reset Ir Reset condi	Close Disable Disable Displa Displa es effect a nternet Ex ts Internet	unused folders ir e script debuggir e script debuggir y a notification a y Accelerator bu after you restart plorer settings Explorer's settir	h History and Favo ng (Internet Explo ng (Other) bout every script tton on selection Internet Explorer Restore	error	ed settings

2. Under Security, select Allow active content to run in files on My Computer.

<ul> <li>Just display the results in the main window</li> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is invalid to the signature on the signature is invalid to the signature on the signature is invalid to the signature on the signature on the signature is invalid to the signature on the signature on the signature of the signature on the signature of the signature on the signature of the signature of the signature of the signature on the signature of the signate of the signature of the signate of the signature of the sign</li></ul>	<ul> <li>Just display the results in the main window</li> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is invol</li> <li>Check for publisher's certificate revocation</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is dc</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable native XMLHTTP support</li> <li>Enable SmartScreen Filter</li> </ul>	<ul> <li>Just display the results in the main window</li> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is invol</li> <li>Check for publisher's certificate revocation</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is dc</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable native XMLHTTP support</li> <li>Enable SmartScreen Filter</li> </ul>	<ul> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is invalid to the signature of the signature is invalid to the signature of the signature of the signature is invalid to the signature of the signatex of the signature of the signature of the signature of the</li></ul>	<ul> <li>Just display the results in the main window</li> <li>Security</li> <li>Allow active content from CDs to run on My Compute</li> <li>Allow active content to run in files on My Compute</li> <li>Allow software to run or install even if the signature</li> </ul>	I
<ul> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is inva</li> <li>Check for publisher's certificate revocation</li> <li>Check for server certificate revocation*</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is dc</li> <li>Enable DOM Storage</li> </ul>	<ul> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is invi</li> <li>Check for publisher's certificate revocation</li> <li>Check for server certificate revocation*</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is dc</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable native XMLHTTP support</li> <li>Enable SmartScreen Filter</li> </ul>	<ul> <li>Security</li> <li>Allow active content from CDs to run on My Computer*</li> <li>Allow active content to run in files on My Computer*</li> <li>Allow software to run or install even if the signature is invol</li> <li>Check for publisher's certificate revocation</li> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browser is dc</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable native XMLHTTP support</li> <li>Enable SmartScreen Filter</li> </ul>	Security Allow active content from CDs to run on My Computer* Allow active content to run in files on My Computer* Allow software to run or install even if the signature is invo Check for publisher's certificate revocation Check for signatures on downloaded programs Check for signatures on downloaded programs Check for signatures on downloaded programs Do not save encrypted pages to disk	<ul> <li>Security</li> <li>Allow active content from CDs to run on My Compute</li> <li>Allow active content to run in files on My Computer</li> <li>Allow software to run or install even if the signature</li> </ul>	I
Enable native XMLHTTP support			et Internet Explorer settings esets Internet Explorer's settings to their default Reset	<ul> <li>Check for signatures on downloaded programs</li> <li>Do not save encrypted pages to disk</li> <li>Empty Temporary Internet Files folder when browse</li> <li>Enable DOM Storage</li> <li>Enable Integrated Windows Authentication*</li> <li>Enable native XMLHTTP support</li> </ul>	
et Internet Explorer settings					set

- 3. Clear Use SSL 3.0.
- 4. If SSL 2.0 is selected, clear it.
- 5. Select Use TLS 1.0, Use TLS 1.1, and Use TLS 1.2.

	et Proper	ties				1
neral	Security	Privacy Co	ntent   Con	nections   Pr	ograms	Advance
otting	_					
etting	5					
	-	Temporary In		folder when	browser	is dc 🔺
		DOM Storag				
		Integrated V				
	and the second second	native XMLH				
	Use S	SmartScreen	1 Filter			
	Use T					
	Use T					
	Use T	S 1.2				
	Vise T	S 1.2 about certifica	ate address	mismatch*		
	Varn Warn				cure mod	ie
	Warn Warn	about certifica	etween secur	re and not se		
	Warn Warn	about certifica if changing be	etween secur	re and not se		
•	Warn Warn Warn	about certific if changing be if POST submi	tween secur	re and not se cted to a zon		
• *Ta	Warn Warn Warn	about certifica if changing be	tween secur	re and not se cted to a zon		
<b>↓</b> *Ta	Warn Warn Warn	about certific if changing be if POST submi	tween secur	re and not se cted to a zon	e that do	es not pe
	Warn Warn Warn	about certifica if changing be if POST submi	etween secur ittal is redired art Internet	e and not se cted to a zon Explorer	e that do	es not pe
eset I	Warn Warn Warn Warn	about certifica if changing be if POST submi after you rest plorer setting	etween secur ittal is redired art Internet	e and not se cted to a zon Explorer Restore ad	e that do vanced s	ettings
eset I Rese	Warn Warn Warn Warn	about certifica if changing be if POST submi	etween secur ittal is redired art Internet	e and not se cted to a zon Explorer Restore ad	e that do	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect of internet Exection.	about certific if changing be if POST submi after you rest plorer setting t Explorer's se	etween secur ittal is redired tart Internet	Explorer Restore add	e that do vanced so Rese	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect of internet Exection.	about certifica if changing be if POST submi after you rest plorer setting	etween secur ittal is redired tart Internet	Explorer Restore add	e that do vanced so Rese	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect of internet Exection.	about certific if changing be if POST submi after you rest plorer setting t Explorer's se	etween secur ittal is redired tart Internet	Explorer Restore add	e that do vanced so Rese	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect of internet Exection.	about certific if changing be if POST submi after you rest plorer setting t Explorer's se	etween secur ittal is redired tart Internet	Explorer Restore add	e that do vanced so Rese	ettings
eset I Rese cond	Warn Warn Warn Warn kes effect of internet Exection.	about certific if changing be if POST submi after you rest plorer setting t Explorer's se	etween secur ittal is redired tart Internet	Explorer Restore add	vanced so Rese ble state	ettings

- 6. Click **OK**.
- 7. Close the Internet Properties window.
- 8. From the Control Panel window, click System and Security > Action Center.

📴 Control Panel	
G O ∞ 📴 + Control Panel +	👻 🕼 Search Control Panel
Adjust your computer's settings	View by: Category 👻
System and Security Prodew your computer's actuals Back up your computer's actuals Back up your computer Prind and fits problems Coose homegroup and sharing We devices and printers Add a deviceWe device and printers We device and printers Add a devicePrograms Uninstall a program	options       User Accounts and Family Safety         options       Setup apendic controls for any user         Appearance and Personalization       Change desktop background         Appearance and Personalization<

9. If the SmartScreen Filter window appears, click OK.

•		rosoft to be checked against a list of reported d will not be used to personally identify you. Fo <u>explorer privacy statement</u> .	r
		OK Cance	4
D Ho	v does SmartScreen Filter help protect i	رکا	

- **10.** Click **All Programs > Internet Explorer**.
- **11.** If the **Set Up Windows Internet Explorer 8** window appears, click **Next**.
- **12.** In the **Turn on Suggested Sites** window, click **No, don't turn on**, and then click **Next**.

et Up Windows Internet Explorer 8	
Turn on Suggested Sites	
Do you want to discover websites you might like based o you've visited?	n websites
Yes, turn on Suggested Sites     No, don't turn on	
Suggested Sites is an online service that uses your browsing history to website suggestions. You can turn off Suggested Sites at any time.	nake personalized
Produko Internet Funderer Driver Statement soline	lext Cancel

**13.** In the **Choose your settings** window, click **Use express settings**, and then click **Finish**.

Set Up Windows Internet Explorer 8	×
Choose your settings	
Before you get started, do you want to:	
<ul> <li>Use express settings Search provider: Bing Search Updates: Download provider updates Accelerators: Blog with Windows Live, Map with Bing, E-mail with Windows Live, Translate with Bing SmartScreen Filter: Enabled Compatibility View: Use updates</li> </ul>	
Choose custom settings Review and modify each setting individually.	
Read the Internet Explorer Privacy Statement online Back Einish Cancel	

**14.** When an error indicates that an Internet connection is not established, close Internet Explorer.



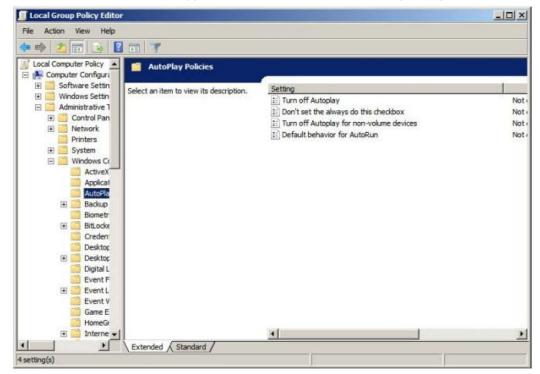
**Note:** After configuring Internet Explorer settings, disable the autoexecute feature.

## Disabling the auto-execute feature

The SVP requires the Windows AutoPlay feature be turned off.

#### Procedure

1. Click Start > Run, and then type gpedit.msc to start the Group Policy Editor.



- 2. Click Local Computer Policy > Computer Configuration, click Administrative Templates > Windows Components, and then click AutoPlay Policies.
- **3.** From the items on the right, double-click **Turn off Autoplay**.

💭 Turn off Autoplay		
Turn off Autoplay	1	Previous Setting Next Setting
• Not Configured	Comment:	
C Enabled		
C Disabled	ansonand	<u>*</u>
	Supported on:	At least Windows 2000
Options:		Help:
Turn off Autoplay on	ε	Turns off the Autoplay feature.         Autoplay begins reading from a drive as soon as you insert media in the drive. As a result, the setup file of programs and the music on audio media start immediately.         Prior to XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.         Starting with XP SP2, Autoplay is enabled for removable drives as well, including ZIP drives and some USB Mass Storage devices.         If you enable this setting, you can disable Autoplay on CD-ROM and removable media drives, or disable Autoplay on all drives.         This setting disables Autoplay on additional types of drives. You cannot use this setting to enable Autoplay on drives on which it is disabled by default.
Start 🙆 🚞		/ 璭 💊 🛛 💀 🖗 🕼

4. In the **Property** window, click **Enabled** and select **All drives**, and then click **OK**.

and the second of the second			
Turn off Autoplay			Previous Setting Next Setting
Not <u>C</u> onfigured	Comment:		
Enabled			
Disabled			
	Supported on:	At least Windows 2000	
ptions:		1	Help:
urn off Autoplay on:			Turns off the Autoplay feature.
II drives			Autoplay begins reading from a drive as soon as you insert media in the drive As a result, the setup file of programs and the music on audio media start immediately.
			Prior to XP SP2, Autoplay is disabled by default on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.
			Starting with XP SP2, Autoplay is enabled for removable drives as well, including ZIP drives and some USB Mass Storage devices.
			If you enable this setting, you can disable Autoplay on CD-ROM and removable media drives, or disable Autoplay on all drives.
			This setting disables Autoplay on additional types of drives. You cannot use

**5.** Close the Group Policy Editor.

- 6. Click Control Panel > Autoplay.
- 7. Clear Use Autoplay for all media and devices, and then click Save.



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

## **Configuring the Registry**

Use Regedit to edit the Windows Registry on the SVP.

### Procedure

- 1. Disable anonymous logon (null connection):
  - a. Click **Start > Run**, and then type regedit and press **Enter**.

🚮 Registry Editor				<u> </u>
File Edit View Favorites Help	Name	Туре	Data	
HKEY_CURRENT_CONFIG				
Computer				ŀ

- b. In the **User Account Control** menu, click **Yes** to open the **Registry Editor** window.
- c. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control \Lsa.

File Edit View	Favori	tes Help			
		🖌 FileSystemU 🔺	Name	Туре	Data
	Ē.	FontAssoc	(Default)	REG_SZ	(value not set)
	<u>+</u>	GraphicsDriv	30 auditbasedirectories	REG_DWORD	0x00000000 (0)
		GroupOrderi	300 auditbaseobjects	REG_DWORD	0x00000000 (0)
	÷.	HAL	ab Authentication Packa	REG MULTI SZ	msv1 0
		hivelist	Bounds	REG BINARY	00 30 00 00 00 20
	<b>.</b>	IDConfigDB	100 crashonauditfail	REG DWORD	0x00000000 (0)
	<b>H</b>	Keyboard La	300 disabledomaincreds	REG DWORD	0x00000000 (0)
	<b>.</b>	Keyboard La	everyoneincludesano	REG DWORD	0x00000000 (0)
	<b>.</b>	Lsa	100 forceguest	REG DWORD	0x00000000 (0)
	<b>+</b>	LsaExtension	100 fullprivilegeauditing	REG BINARY	00
			100 LimitBlankPasswordUse	REG DWORD	0x00000001(1)
	÷	MediaCateg	10 LsaPid	REG DWORD	0x000001f8 (504)
	÷	MediaInterfa	NoLmHash	REG DWORD	0x00000001 (1)
	÷	MediaProper	ab Notification Packages	REG MULTI SZ	scecli
	÷.	MediaTypes	ProductType	REG DWORD	0x0000006 (6)
	÷	MobilePC	Restrictanonymous	REG_DWORD	0x00000000 (0)
		MPDEV	100 restrictanonymoussam	REG DWORD	0x00000001 (1)
	÷	MSDTC	eine eine eine eine eine eine eine eine		0.00000001(1)

d. Double-click **restrictanonymous**.

		Name	Туре	Data
	Edit DWORD (32-bit) Valu Value name: restrictanonymous Value data:	Base	ORD ORD LTI_SZ ARY ORD	(value not set) 0x00000000 (0) 0x00000000 (0) msv1_0 00 30 00 00 00 20 0x00000000 (0)
	1	Hexadecimal     Decimal     OK     Car	ncel ORD	0x00000000 (0) 0x00000000 (0) 0x00000000 (0) 00 0x00000000 (1)
41	MediaDRM     MediaInterfa     MediaProper     MediaTypes     MobilePC     MPDEV     MSDTC	NoLmHash Notification Packages ProductType restrictanonymous	REG_DWORD REG_DWORD REG_MULTI_SZ REG_DWORD REG_DWORD REG_DWORD	0x000001f8 (504) 0x00000001 (1) scecli 0x00000006 (6) 0x00000000 (0) 0x00000000 (1)

- e. Set Value data to 1, verify Hexadecimal is selected, and then click OK.
- 2. Disable the beep when Remote Desktop Connection is connected:
  - a. In the **Registry Editor** window, navigate to HKEY_LOCAL_MACHINE\System \CurrentControlSet\Control\Terminal Server.
  - b. In the **Edit** menu, click **New** > **DWORD (32-bit) Value**.
  - c. Type DisableBeep.

	Session Man	Name	Туре	Data
		(Default)	REG SZ	(value not set)
	SQMServicel	AllowRemoteRPC	REG DWORD	0x00000000 (0)
÷	- Srp	100 DelayConMgrTimeout	REG DWORD	0x00000000 (0)
	SrpExtension	BillipeleteTempDirsOnExit	REG DWORD	0x00000001 (1)
Ē	- 📙 StillImage	100 fDenyTSConnections	REG DWORD	0x00000000 (0)
	- 🚽 Storage	100 fSingleSessionPerUser	REG DWORD	0x00000001 (1)
	- SystemInfor	ab InstanceID	REG SZ	15260f9d-f1fb-46b9
Ē		NotificationTimeOut	REG DWORD	0x00000000 (0)
		RerSessionTempDir	REG DWORD	0x00000000 (0)
±		ab ProductVersion	REG SZ	5.1
	TimeZoneInf	ab RCDependentServices	REG MULTI SZ	CertPropSvc Session
		ab SnapshotMonitors	REG SZ	1
		38 StartRCM	REG DWORD	0x00000000 (0)
		10 TSAdvertise	REG DWORD	0x00000000 (0)
		100 TSUserEnabled	REG DWORD	0x00000000 (0)
		DisableBeep	REG DWORD	0x00000000 (0)
· · · · ·				
		-		•

### d. Double-click **DisableBeep**.

	🖳 📔 Session Man 🔺	Name	Туре	Data
Edit DWORD (32	2-bit) Value	×	REG_SZ REG_DWORD	(value not set) 0x00000000 (0)
Value name:			REG_DWORD	0x00000000 (0)
DisableBeep			REG_DWORD	0x00000001 (1)
Value data:	- Bas		REG_DWORD	0x00000000 (0)
			REG_DWORD	0x0000001(1)
1		Transis Solition	REG_SZ	15260f9d-f1fb-46b9
	C	Decimal	REG_DWORD	0x00000000 (0)
			REG_DWORD	0x00000000 (0)
		OK Cancel	REG_SZ	5.1
			REG_MULTI_SZ	CertPropSvc Session
	usbstor	A SnapshotMonitors	REG_SZ	1
		38 StartRCM	REG_DWORD	0x00000000 (0)
		100 TSAdvertise	REG_DWORD	0x00000000 (0)
		TSUserEnabled	REG_DWORD	0x00000000 (0)
I I I T	Wdf	DisableBeep	REG_DWORD	0x00000000 (0)
<pre>4[ ' ' ' '</pre>				•

- e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.
- **3.** Configure Remote Desktop Connection:
  - a. In the **Registry Editor** window, navigate to HKEY_LOCAL_MACHINE\SOFTWARE \Policies\Microsoft\Windows NT\Terminal Services.

SOFTWARE	Name	Туре	Data
Image: Construction of the second	(Default)	REG_SZ	(value not set) 0x00000000 (0)

- b. In the **Edit** menu, click **New** > **DWORD** (32-bit) Value.
- c. Type fPromptForPassword.
- d. Double-click **fPromptForPassword**.
- e. Set **Value data** to 1, verify Hexadecimal is selected, and then click **OK**.

	SOFTWARE	Name	Type	Data
E E E E E E E E E E E	ATT Technolonies dit DWORD (32-bit) Value Value name: [FPromptForPassword Value data: 1] rols tal Controls settings. Windows Windows NT Terminal Windows	Base Hexadecimal Decimal	Ancel	(value not set) 0x00000000 (0)

- f. In the **Edit** menu, click **New** > **DWORD** (32-bit) Value.
- g. Type SecurityLayer.

SOFTWARE	Name	Type	Data
Image: Construction of the second	(Default)	REG_SZ REG_DWORD REG_DWORD	(value not set) 0x00000001 (1) 0x00000000 (0)

4. Restart the server.

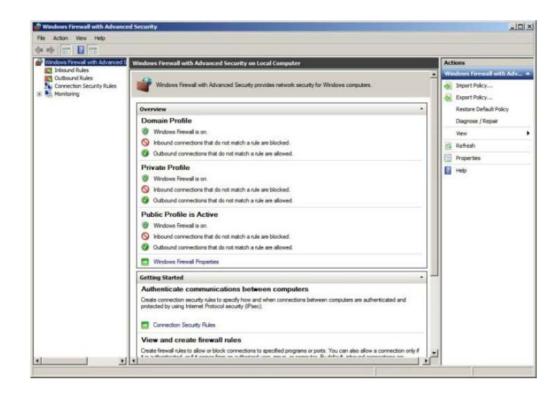
**Note:** After configuring the Registry, enable ICMP (ping) reply.

## Enabling ICMP (ping) reply

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

#### Procedure

1. Click Control Panel > Administrative Tools, and then start Windows Firewall with Advanced Security.



2. In the left pane, click Inbound Rules.

Windows Firewall with Advanced S	Inbound Rules					Actions
Cutbound Rules	Name	Group +	Profile	Enabled	Ac +	Indexed Rates
Connection Security Rules	Core Networking - Internet Group Management Protoc	Core Networking	Al	Yes	Alle	13 New Rule
Manitoring	Core Networking - IPHTTPS (TCP-In)	Core Networking	Al	Yes	Alk	The second se
S. Carriero de	Core Networking - IPv6 (IPv6-In)	Core Networking	Al	Yes	Allı	V Filter by Profile
	Core Networking - Multicast Listener Done (ICMPv6-In)	Core Networking	Al	Yes	Alt	Filter by State
	Core Networking - Multicast Listener Query (ICMPv6-In)	Core Networking	Al	Yes	Alic	
	Core Networking - Multicast Listener Report (ICMPv6-In)	Core Networking	AB	Yes	Aå	Titter by Group
	Core Networking - Multicast Listener Report v2 (ICMPv	Core Networking	AB	Yes	Alt	View
	Core Networking - Neighbor Discovery Advertisement (	Core Networking	AL	Yes	Abc	The second second
	Core Networking - Neighbor Discovery Solicitation (ICM	Core Networking	Al	Yes	Ali	<u>Ci</u> Refresh
	Core Networking - Packet Too Big (JCMPv6-br)	Core Networking	Al	Yes	Ab	Export List
	Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	Al	Yes	Abc	Heb
	Core Networking - Router Advertisement (ICMPvti-In)	Core Networking	Al	Yes	Alk	E nep
	Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	Al	Yes	Alt	
	Core Networking - Teredo (UDP-In)	Core Networking	AL	Yes	Alic	
	Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	AL	Yes	Alk	1
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coordi	Domain	No	Alt	1
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coord	Privat	No	Ali	
	Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coord	Domain	No	Alle	1
	Distributed Transaction Coordinator (RPC-EPMAP)	Detributed Transaction Coord	Privat	140	Alt	1
	Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coord	Privat	No	Abr	1
	Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coordi	Domain	No	Ab	1
	File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	No	Alt	1
	File and Printer Sharing (Echo Request - ICHPv4-In)	File and Printer Sharing	Privat	No	Abr	1
	File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Privat	No	ASt	1
	File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No	Abi	1
	File and Printer Sharing (LLMVR-LOP-In)	File and Printer Sharing	Al	No	Alle	1
	File and Printer Sharing (H8-Datagram-In)	File and Printer Sharing	Doman	No	Alt	1
	File and Printer Sharing (H8-Datagram-In)	File and Printer Sharing	Privat	No	ABr	1
	File and Printer Sharing (NE-Name-In)	File and Printer Sharing	Domain	No	Alt	1
	File and Printer Sharing (H8-Name-In)	File and Printer Sharing	Privat	No	Alt	1
	File and Printer Sharing (NE-Session-In)	File and Printer Sharing	Privat	No	Alc	1
	File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No	Alt	1
	File and Printer Sharing (SME-In)	File and Printer Sharing	Domain	No	Alt -	
	File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No	Alt	

- 3. Click all the following inbound rules, and then right-click and click **Enable Rules**.
  - File and Printer Sharing (Echo Request ICMPv4-In) (Profile=Domain)
  - File and Printer Sharing (Echo Request ICMPv4-In) (Profile=Private)

- File and Printer Sharing (Echo Request ICMPv6-In) (Profile=Domain)
- File and Printer Sharing (Echo Request ICMPv6-In) (Profile=Private)

Windows Firewall with Advanced S	Inbound Rules					Actions
Inbound Rules	Name	Group +	Profile	Enabled	Act	Inbound Rales
Connection Security Rules	Core Networking - Multicast Listener Done (ICMPv6-In)	Core Networking	Al	Yes	Allo	New Rule
Manitoring	Core Networking - Multicast Listener Query (ICMPv6-In)	Core Networking	Al	Yes	Allo	
- Contracting	Core Networking - Multicast Listener Report (ICMPv6-In)	Core Networking	All	Yes	Alio	V Filter by Profile
	Core Networking - Multicast Listener Report v2 (ICMPv	Core Networking	AB	Yes	Allo .	V Filter by State
	Core Networking - Neighbor Discovery Advertisement	Core Networking	Al	Yes	Allo	
	Core Networking - Neighbor Discovery Solicitation (IC	Core Networking	Al	Yes	Allo	Y Filter by Group
	Core Networking - Packet Too Big ()CMPv6-In)	Core Networking	Al	Yes	Allo	Ves
	Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	All	Yes	Allo	10
	Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	AB	Yes	Alo	Ci Refresh
	Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	Al	Yes	Alo_	Export List
	Core Networking - Teredo (UDP-In)	Core Networking	AB	Yes	Aão	Heb
	Core Networking - Time Exceeded (ICMPv6-3n)	Core Networking	AZ	Yes	Alio	La rep
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coordi	Domain	No	Allo	Selected Items
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coordi	Privat	No	Allo	Next Prove Distance of Concerns
	Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coord	Domain	No	Allo	Disable Rule
	Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coord	Privat	No	Allo	& Cut
	Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coordi	Privat	No	Allo	
	Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coord	Domain	No	Allo	Copy
	File and Printer Sharing (Echo Request - 1049v4-In)	File and Printer Sharing	Domain	Yes	Allo	X Delete
	File and Printer Sharing (Echo Request - ICHPv4-In)	File and Printer Sharing	Privat	Yes	Ale	Help
	File and Printer Sharing (Echo Request - ICHPv6-In)	File and Printer Sharing	Privat	Tes	All	E rep
	File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	Yes	ALC	
	File and Printer Sharing (LLMNR-UCP-In)	File and Printer Sharing	Al	No	Allo	
	File and Printer Sharing (NE-Datagram-In)	File and Printer Sharing	Domain	No	Allo	
	File and Printer Sharing (HE-Datagram-In)	File and Printer Sharing	Privat	No	Allo	
	File and Printer Sharing (NE-Name-In)	File and Printer Sharing	Domain	No	Allo	
	File and Printer Sharing (16-Name-In)	File and Printer Sharing	Privat	No	Allo	
	File and Printer Sharing (18-Session-In)	File and Printer Sharing	Privat	No	Allo	1
	Pile and Printer Sharing (N8-Sesson-In)	File and Printer Sharing	Domain	No	Allo	1
	File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No	Allo	1
	File and Printer Sharing (SME-In)	File and Printer Sharing	Privat	No	Allo	1
	File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Domain	No	Alio	1
	File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Privat	No	Alo -1	1
1 1	1				2	

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

### Changing the computer name

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

#### Procedure

- 1. Click Control Panel > System, and then click Change settings under Computer name, domain, and workgroup settings.
- 2. In the System Properties window, click the Computer Name tab, and then click Change.

omputer description:	
	For example: "Kitchen Computer" or "Mary's Computer".
ull computer name:	User-PC
Vorkgroup:	WORKGROUP
o use a wizard to join letwork ID.	a domain or workgroup, click Network ID
o rename this comput orkgroup, click Chan	ter or change its domain or Change

**3.** In the **Computer Name** field, type SVP-PC.

omput	n change the name and the membership of this er. Changes might affect access to network resources. <u>formation</u>	computer
10000	ter name:	- flany's
SVP-P		
SVP-P	nputer name: C	
	More	
Memb	per of	
0	Domain:	
		inge
œ	Workgroup:	
	WORKGROUP	
	OK Cancel	

**4.** When prompted to restart your computer, click **OK**.

computer. Changes might affect an More information Computer name:			mputer to apply these
SVP-PC	Before resta	rting, save any o	open files and close all programs.
Full computer name: SVP-PC			ок
	More	prk ID	or this Display
Member of			
C Domain:			r restarting this computer)
		inge	a restarting this computery
Workgroup:			
WORKGROUP			
	-11		
	OK Cancel	1	
		-	
	OK Cancel	Apply	1

5. Click Close.

Computer description:		
	For example: "Kitchen Compu Computer".	iter" or "Mary's
full computer name:	SVP-PC	
Vorkgroup:	WORKGROUP	
fo use a wizard to join a Network ID.	a domain or workgroup, click	Network ID
To rename this compute vorkgroup, click Chang	er or change its domain or le.	Change

6. Click Restart Now.

Microsoft Windows		×
You must restart	your computer to apply th	ese changes
Before restarting, sa	ive any open files and close all	programs.
	Restart Now	Restart Later

**7.** Wait for the server to restart.

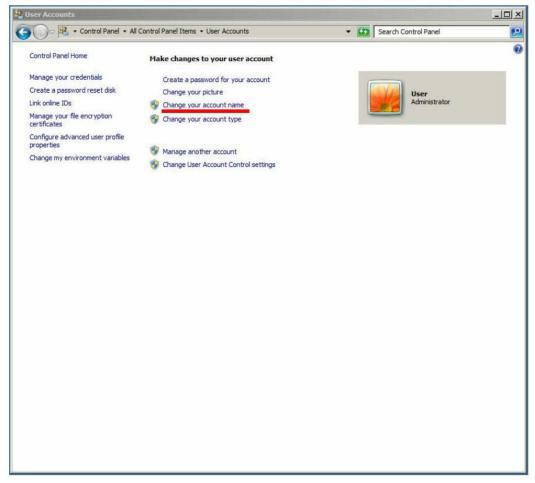
**Note:** After changing the computer name, change the account name.

### Changing the account name

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

#### Procedure

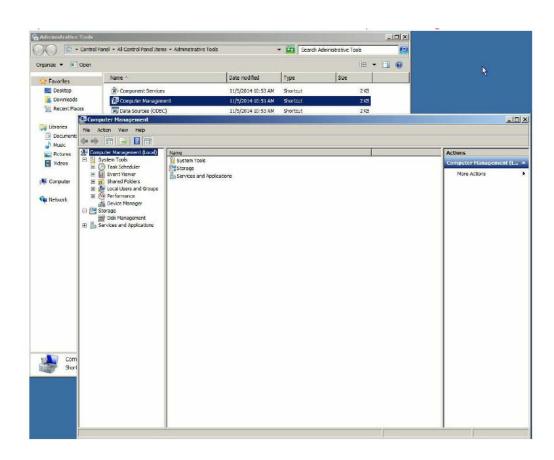
1. Click Control Panel > User Accounts, and then click Change your account name.



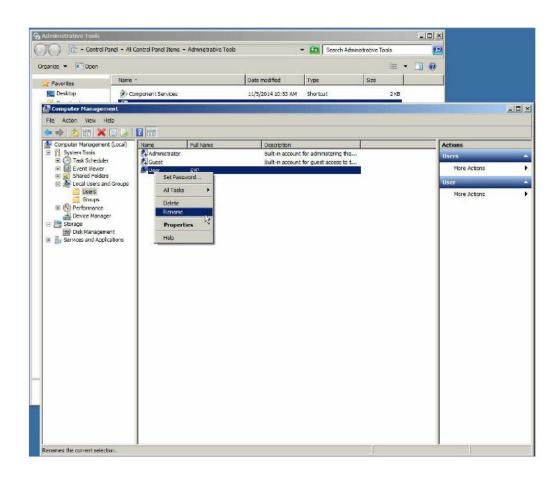
2. Type SVP for the new account name, and then click Change Name.

and the change Your Name	
🚱 🕞 🕫 🔹 Control Panel 🔹 All Control Panel Items 🔹 User Accounts 🔹 Change Your Name 🔹 😨 Search Control Panel	<b>1</b>
Type a new account name User Administrator	
SVP This name will appear on the Welcome screen and on the Start menu.	
Change Name Cancel	

- **3.** Close the **User Accounts** window.
- 4. Click Control Panel > Administrative Tools, and then click Computer Management.



- 5. Click Computer Management (Local) > System Tools, and then click Local Users and Groups > Users.
- 6. In the right window, right-click **User**, and then click **Rename**.



7. Rename User to SVP.

	ol Panel 🔹 All Contro	a ranei sterits	A DISTRICT OF THE		• Mail Search	Administrative Tools	
ganize 💌 💽 Open				1	1	/Ⅲ ▼ [	<b>1</b> • •
Favorites	Name +			Date modified	Туре	Size	
Desktop	Compon	ent Services		11/5/2014 10:53 AN	I Shortcut	2 KB	
Computer Hanag							
File Action View							
	K 🖻 🕒 🔽			(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)			
System Tools	ient (Local) Ner	me Administrator	FullName	Description Built-in accou	nt for administering t	the	Actions
🖽 🕐 Task Sched	uler 🛃	Guest			nt for guest access t		Users
E 🛃 Event View	er 🍠	SVP	SVP		All Provide State		More Actions
E 😹 Local Users							User
Groupe							More Actions
E ( Performance							
E 🚰 Storage	2005						
Disk Manag	ement						
() 10 se has sign							

8. Close the **Computer Management** window, and then close the **Administrative Tools** window.



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

### Configuring the password setting for Administrator

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

#### Procedure

1. Click Control Panel > Administrative Tools, and then click Computer Management.

Administrative	Took					_10	×	
00 .	Control Panel - All Control Panel Item	s - Administrative Tools		🕶 🚮 🛛 Search A	Administrative Too	ols		
Organize •	Open					HE + 🔟 🌘	2	10
😤 Favorites	Name +	1	Date modified	Туре	Size			k
E Desktop	A- Component Service		11/5/2014 10:53 AM	Shortcut		2 KB		
😹 Downloads	🔁 Computer Managem	ent	11/5/2014 10:51 AM	Shortnut		2 KB		
🔛 Recent Plac	Cheere see ces less.	.)	11/5/2014 10:53 AM	Shortcut		2.KB		
-	Computer Management							
Cibraries	File Action View Help							
Music								
Pictures	Computer Management (Local)	Name						Actions
Videos	E 🔀 System Tools E 🕑 Task Scheduler	System Tools						Computer Management (L., 🔺
-	🗉 🔝 Event Viewer	Services and Application	6					More Actions
🖳 Computer	E and Shared Folders E and Groups							
Network	E 🚳 Performance							
6-	Device Manager							
	Disk Management							
	E Services and Applications							
Com								
Short Short								
						1		

- 2. Click Computer Management (Local) > System Tools, and then click Local Users and Groups > Users.
- **3.** In the right window, right-click **Administrator**, and then click **Set Password**.
- 4. In the warning message, click **Proceed**.

Set Pase	sword for Administrator	×
	Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user's password is reset.	
	This data loss will occur the next time the user logs off.	
	You should use this command only if a user has forgotten his or her password and does not have a password reset disk. If this user has created a password reset disk, then he o she should use that disk to set the password.	r
	If the user knows the password and wants to change it, he or she should log in, then press CTRL+ALT+DELETE and click Change Password.	
	For additional information, click Help.	
	Proceed Cancel Help	

- 5. In the **New password** and **Confirm password** fields, type the administrator password raid-login.
- 6. Click **OK**.

New password:		
Local	Users and Groups	×
Confirm pass ff you cl This use files, stc	The password has been set.	encrypted
f you click C	ОК	ata loss wil

- 7. Close the **Computer Management** window, and then close the **Administrative Tools** window.
- 8. Restart Windows.

Ē

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

### Changing the password setting

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

#### Procedure

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

a Create Your Password				<u>_     ×</u>
S + All Control Panel Items + User Accounts + Create Your Password	•	-	Search Control Panel	
Create a password for your account				
If your password contains capital letters, they must be typed the same way of How to create a strong password	every tim	e you	log cn.	
Type a password hint The password hint will be visible to everyone who uses this computer. What is a password hint?				
	Cr	eate p	assword Cancel	

- 4. Click Create password.
- 5. Close the window.

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

### Installing the SVP software

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

#### Procedure

- **1.** Obtain the appropriate SVP ISO image for your storage system from the firmware distribution set. Verify the ISO image corresponds to the firmware currently running on the storage system.
- **2.** Download the SVP ISO from TISC to the CE notebook, and then use an ISO reader to mount the SVP ISO as the next available drive letter.
- 3. Launch Remote Desktop Connection and click the **Show Options** drop-down menu.



4. Click the Local Resources tab, and then click More.

260	Connection
eneral   D	isplay Local Resources Programs Experience Advance
Remote al.	udio Configure remote audio settings. Settings
Keyboard	Apply Windows key combinations:
V	Only when using the full screen
.ocal devi	ces and resources
-	Choose the devices and resources that you want to use in your remote session.
	Printers Clipboard
	Mor

- **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.

Computer 💭							-	. 🗆 >
GO + Computer	*				• 🔛 Search Computer			
Organize 🔻 System proper	ties Uninstall or change a program Ma	p network drive Open Control Panel				11 h	• 🗖	
E 🚖 Favorites E Desktop Downloads E Recent Places	Hard Disk Drives (1)      Local Disk (C:)      78.5 GB free of 99.8 GB      Devices with Removable Storage (2)							
<ul> <li>□ □ Libraries</li> <li>□ □ Documents</li> <li>□ ↓ Music</li> <li>□ □ Pictures</li> <li>① □ Videos</li> </ul>	Floppy Disk Drive (A:)	DVD Drive (D:) 0 bytes free of 0 votescely CDFS	DKCMAIN_SVP_8 1.02 GB	3303				
Computer Coll Disk (C:) Coll Disk (C:) Coll Disk (D:) DKCMA Coll Disk (D:) DKCMA Coll Disk (D:) DKCMA								
🗄 📬 Network								
	kgroup: WORKGROUP Memo ccessor: Intel(R) Xeon(R) CPU E5	ry: 8.00 GB						_
E on USSCC-RMEJIA2								
😋 🔾 🖓 🗣 🔹 Computer	✓ E on USSCC-RMEJIA2				👻 🔛 🛛 Search E on USSC	C-RMEJIA2		
Organize 🔻						38	• 🔟	
🖂 🚖 Favorites	Name *	Date modified	Туре	Size				
E Desktop	📕 firmware	1/13/2016 11:22 PM	File folder					
Downloads	鷆 oss	1/13/2016 11:22 PM	File folder					
🔛 Recent Places	RaidManager	1/13/2016 11:22 PM	File folder					
and the second second second	Setup2K	1/13/2016 11:22 PM	File folder					
E 🔚 Libraries	Software	1/13/2016 11:22 PM	File folder					
	tool	1/13/2016 11:22 PM	File folder					
E Pictures	Setup	1/13/2016 11:08 AM	Application	60 KB				
E Videos	$\smile$							
E 📑 <u>Computer</u> E 💒 Lo&Disk (C:)								
DVD Drive (D:) DKCMA     E on USSCC-RMEJIA2								
🗄 📬 Network								
7 items								_

- 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.

			Hitachi De	evice Manager - St	orage Navigator			×
Environme	ntal Settir	ngs				0/2/		HITACHI
Please input the II	P address of the s	5VP before updating the	e firmware or the soft	ware of the storage syste	em,			
SVP IP Address:	IPv4	IPv6		ware of the storage syst	en.			
							Apply	Cancel

- 11. Click Apply.
- **12.** Add the storage system.

🐅 Hitachi Device Manager - Storage Navigator			_ 🗆 ×
Environmental Settings			HITACHI
In the case of adding the storage system, push [Add] button. In the case of changing the target of update, select the storage In the case of editing the setting of the storage system, select th	systems and push [Selec he storage system and p	st Update Objects] button. ush [Edit] button. Push [Apply] button for executing setup.	
	Add System Set values for the new	System and click [Apply] to confirm.	Refresh
Storage Systems			
Select All	System Selection:	Auto Discovery	
System Name Type	IP Address (CTL1):	● IPv4 ○ IPv6	sion (Storage System)
	IP Address (CTL2):	IPv4  IPv6	
	System Name:	VSP 6800 (Max, 180 characters)	
	Description:	VSP 6800	
		(Max, 180 characters, or blank)	
	User Name:	maintenance (Max, 256 characters)	
	Password:		
Add Select Update Objects Edit	Not start service a	fter addition immediately	Selected: 0 of 0
Concercificate Collects		Apply Cancel	
			Apply Cancel

**13.** Register the storage system.

	al Settings		· `	
the case of changing	he storage system, push [Add] button. g the target of update, select the stora he setting of the storage system, select	age systems and push [Sel	ect Update Objects] button. push [Edit] button. Push [Apply] button for executin	
Storage Sys	tems			Refresh
Select All				
System Name	Type	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
VSPG800	VSP G800 and VSP F800	XXXXXXXXX	-> 83-03-02-60/00	83-03-01-60/00 -> 83-03-02-60/00
Add Se	Noct Update Objects	Remove		Selected: 0 of 1

**14.** Click the storage system.

You are presented with the following two options:

- Upgrading the firmware and adding the storage system
- Adding the storage system without upgrading the firmware
- **15.** If the storage system firmware is current, click **Select Update Objects** and clear **Firmware (Storage System)**. Doing so adds the storage system without upgrading the firmware.

			e systems and push [Selec t the storage system and pu	ush (Edit) button. Push (Apply) buttor	for executing setup.		Refresh
Storage Syst	tems						
Select All	44				20		
System Name	Ty VSP G800 and VSP	98 Select Update	Serial Number	Software Version (Storage N	lavigator)	Firmware Version (Sto	
		Update:	-	(Storage System)	Cancel		
	lect Update Objects	Edit	Remove				ed: 1 of 1

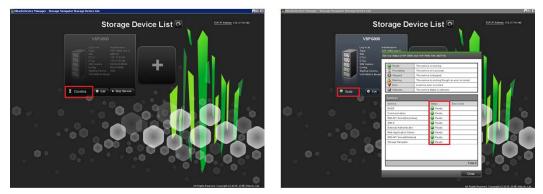
**16.** Click **Apply**, and then click **Confirm** to added the storage system to the SVP.

vironmenta	Settings				НІТА
software update in sh [Update] button fo software and firmwa	progress. r starting the firmware update. are are updated, push [Close] buttor	for exit the Environmenta	I Settings.		
System Name	Туре	Serial Number	Software (Storage Navigator)	Firmwar	re (Storage System)
VSP 0800	VSP G800 and VSP F800	X00000X	Completed	(Not Update)	Update

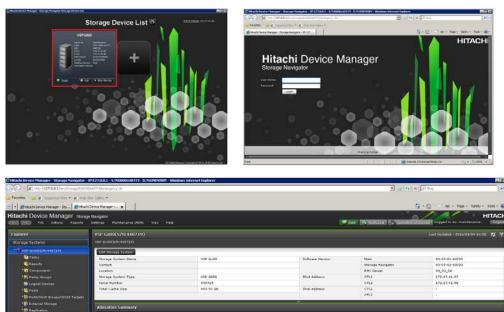
**17.** On the Desktop, click the **Open StorageDevice List** shortcut.



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



**18.** 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.

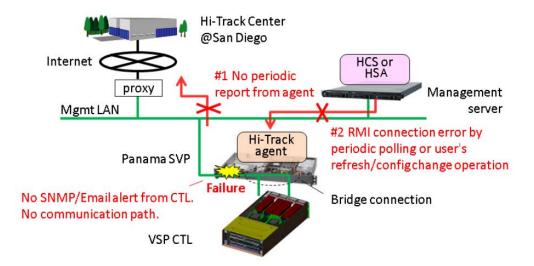
#### Procedure

- **1.** Prepare a master virtual SVP image:
  - a. Create the virtual SVP using the procedure in <u>Configuring the virtual SVP (on page 109)</u>. You do not have to set up the network at this time.
  - b. Configure the SVP guest OS using the procedure in <u>Configuring the SVP guest</u> OS (on page 112).
  - c. Install the SVP using the procedure in <u>Completing the configuration (on page 92)</u>. You do not have to configure the SVP IP address at this time. In addition, do not register a DKC using the Storage Device List.
- **2.** Turn off the master virtual SVP.
- 3. Clone the master virtual SVP, and then start the cloned virtual SVP.
- 4. Configure the Windows OS network information in the cloned virtual SVP.
- **5.** Set the IP address for the SVP. This IP address is used to communicate with the storage system.
- 6. Register a storage system using the Storage Device List.

## **Detecting SVP failures**

SVP failures are detected and resolved using the following methods.

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



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

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

## Setting up the SVP locale

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

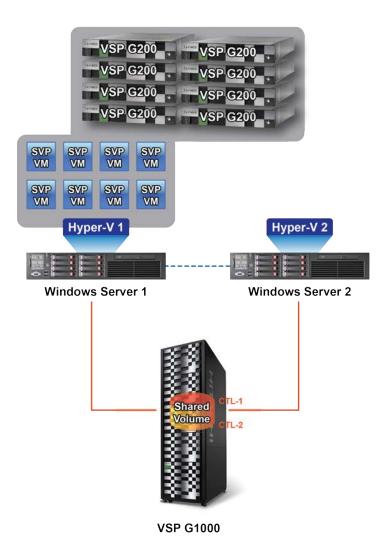
If you intend to install the SVP software using a language other than English and Japanese, change the SVP's locale setting to reflect the appropriate language using the procedure for the Windows version installed on the SVP. For more information, see the instructions for your Windows operating system.

### **Network connection for Hyper-V**

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

Ë

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



# Minimum requirements for Hyper-V Server 2012 R2 VM

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

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

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

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

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

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

### Installing and Configuring Hyper-V on Windows 2012 R2 Server

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

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

#### Procedure

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

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

Re:			Server Manager					^
Serve	er Manager • Das	shboard			• 🕲 I 🧗	Manage Tools	View H	elp
Dashboard     Local Server     All Servers     File and Storage Serv	E Create Virtual S Before You Begin Instalation Type Server Selection Server Roles Features Hyper-V Vytrail Switches	Virtual machines require virtual sw role, you can create virtual machin One virtual switch will be created f at least one virtual switch now to p	eatures Wizard itches to communicate with other core es and attach them to a virtual switch for each network adapter you select. through entropy and the top through the select of the select of the select Description Intel® Thement Controller X540	Ve recommend that you create wity to a physical network. You tual Switch Manager.				
	Migrasi Jakon je Migrasi Jones Defaulti Stores Confirmation Results	Ethernet 2     We recommend that you ress     network adapter, do not select	Intel(R) Ethernet Controller X340 Intel(	AT2	ctivate Windows e to System in Control		Hide	-

**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.

		Server Manager	 		- 0	×
⊖⊙- Serve	er Manager 🔹 Dasl	nboard	• @   <b>/</b> •	danage Tools	View I	Help
Dashboard Local Server All Servers File and Storage Serv	Default Stores Before You Begin Installation Type Server Roles Peatures Hyper-V Virtual Switches Migration Deale Stores Confirmation Results	Add Roles and Features Wizard Hyper-V uses default locations to store virtual hard disk files and virtual m unites you specify different locations when you create the files. You can ch now, or you can change them later by modifying Hyper-V settings. Default location for virtual mard disk files: Ch12ers19/bit/Clocuments/Hyper-V/Virtual Hard Disks Default location for virtual marchine configuration files: Ch3ProgramData/Microsoft/Windows/Hyper-V			Hide	
	BPA results	Previous     Next >     BPA results	ctivate Windows o to System in Control P	anel to activate \		

### 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**.

3	Hitachi Device Manager - Storage Navigator	_ 🗆 X
Hitachi Device	Manager - Storage Navigator	
	Hitachi Device Manager - Storage Navigator	
	Choose Destination Location	
	Select folder where setup will install files.	
	Setup will install Hitachi Device Manager - Storage Navigator in the following folder.	
	To install to this folder, click Next. To install to a different folder, click Browse and select another folder.	
	Destination Folder C:Mapp Browse	
	InstallShield	
	OK. Cancel	

**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**.

172.17.71.246 - Remote Desktop Connection		1777 A. 1977 A.
	VM7_g1 on HYPVSRV-2 - Virtual Machine Connection	
File Action Media Clipboard View Help		
Recycle i 🤹 💿 💿 🥥 🚺 🕪 🏂 🖄		
Environmental Settings		HITACHI
Please input the IP address of the SVP before updating the	e firmware or the software of the storage system.	
SVP IP Address		
172-17,71-253		
		=
	Activat	a Ministerio
	A	cancel

5. Complete the fields in the Add System window.

Action Media Clipboard View H			
vironmental Settings			• HITA
he case of adding the storage system, push	[Add] button.		
he case of changing the target of update, se he case of editing the setting of the storage	Add System		
	Set values for the new	System and click [Apply] to confirm.	
Storage Systems	System Selection:	Auto Discovery     Manual	Refresh
Select All	IP Address (CTL1):	IPv4     IPv6	
System Name Type	IP Address (CTL2):	172.17.42.231 IPv4	irmware Version (Storage System)
	IP Address (CTC2).	172.17.42.232	
			-21
	System Name:	HM800_42.231	
		(Max, 180 characters)	
	Description:		
		( Max, 180 characters, or blank )	
	User Name:	maintenance	
	User Name:	(Max, 258 characters)	×
	Password:	(Max, 256 characters )	
	Not start service a	(Max, 200 characters ) fter addition immediately	
Add Select Update Objects	5	Apply Cancel	Selected: 0 of 0

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

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

not select **Manual** to set it.

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

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

the case of changing t	storage system, push [Add] but the target of update, select the s	Bon.	dast Hadata Objected hadron	
		lorage systems and push [S	elect opeane objectsj button.	
the case of editing the	setting of the storage system, s	select the storage system an	d push (Edit) button. Push (Apply) button for executi	ing setup.
				Refret
Storage Syste	ems			
Select All	proposition -			1174 C
System Name	Type VSP 0200	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System 83-04-02-20:00 -> 83-04-02-20:02
		d. control		
Add	et Updure Ocietta			

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**

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



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



**Note:** Before upgrading the SVP software:

- Back up your SVP configuration. For details about backing up your SVP configuration, see <u>Backing up the SVP configuration (on page 248)</u>.
- Disable the Hi-Track Remote Monitoring System. Otherwise, the upgrade procedure fails. You can enable Hi-Track after you upgrade the SVP software using Storage Device List.
- View all active alerts (see <u>https://support.hitachivantara.com/en_us/</u> <u>contact-us.html</u>).

### Stopping the service in each storage system

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

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

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

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

#### Procedure

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

Chapter 9: Upgrading the SVP software

Note: When the storage system with **S/W Version** 83-01-xx or later is registered, set all the registered storage systems so that they do not start services automatically when restarting the SVP. For more information, see <u>Changing storage system information in the Storage Device List (on page 210)</u>.



The Stop Service screen opens.

Stop Servi	ce		
i	Please confir	m to stop service	r.
		Confirm	Cancel

2. Click Confirm.

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

# Upgrading the SVP software only

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

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

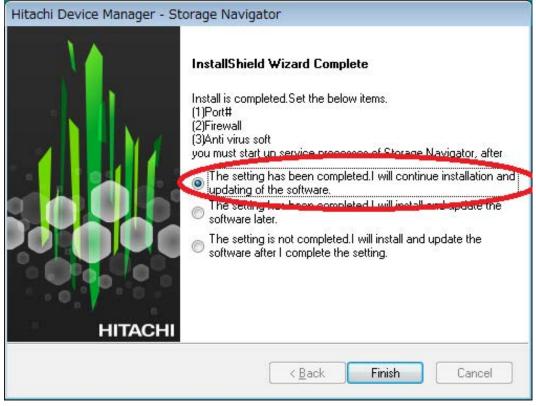
Chapter 9: Upgrading the SVP software

**Note:** Before upgrading the SVP software:

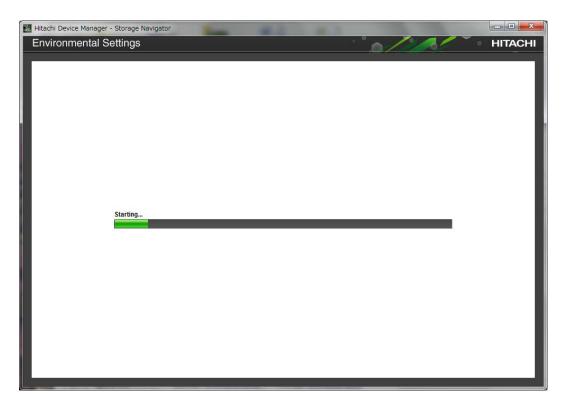
- Disable the Hi-Track Remote Monitoring System (see <u>http://</u><u>hitrack.hds.com</u>); otherwise, the upgrade procedure will fail. You can enable Hi-Track after you upgrade the SVP software.
- View all active alerts (see <u>https://support.hitachivantara.com/en_us/</u> <u>contact-us.html</u>).

#### Procedure

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



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



- **5.** Wait for the preparation to complete and for the target storage systems list window to open.
- **6.** When the target storage systems list window opens, select the appropriate storage systems, and then click **Select Update Objects**.

twironmental S the case of adding the stor the case of changing the ta				HITA
he case of changing the ta				
he case of changing the ta				
	arget of update, se	lect the storage syste	ems and push [Select Setup Object] button.	
he case of editing the sett	ting of the storage	system, select the st	orage system and push [Edit] button. Push [Apply] button	for executing setup.
				Refresh
0	2			
Storage Systems	5			
Select All				
System Name	Туре	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
unit0	VSP G800	300001	83-01-03-60/00 -> 83-01-20-60/02	83-01-20-60/00 -> 83-01-20-60/02
Add Select U	pdate Objects	Edit Rei	move	Selected: 1 of 1

The Select Update Objects window opens.

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

Chapter 9: Upgrading the SVP software

Select Update Object	ts		
Check the update o	bject and click Apply to confirm.		
Update:	Software (Storage Navigator)		
		Apply	Cancel

### 8. Click Apply.

The **Update software and firmware** window opens.

#### 9. Click Confirm.

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

Environmental Settings HITACI	-11
Push [Update] button for starting the firmware update.	
Push [Update] button for starting the firmware update.	
r ush (opcate) buttor for starting the inniviate opcate.	
All software and firmware are updated, push [Close] button for exit the Environmental Settings.	
System Name Type Serial Number Software (Storage Navigator) Firmware (Storage System)	
Storage1 VSP 0800 400102 Inprogress	
Close	

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

iitachi Device Manager Environmental		ator			
The software update in pro Push [Update] button for s All software and firmware	ogress. Larting the firmware are updated, push	update. [Close] button for exit the Environme	ntal Settings.		
System Name	Туре	Serial Number	Software (Storage Navigator)	Firmwa	are (Storage System)
Storage1	VSP 6800	400102 Dinprogres		(Select Update)	Update

The following table shows the possible status conditions:

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

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

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

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

#### **Before you begin**

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

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



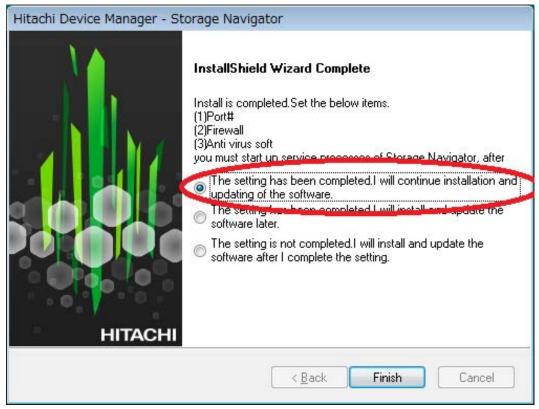
**Note:** This upgrade time is approximately 3.5 hours for storage systems with firmware version 83-01-21 or later.



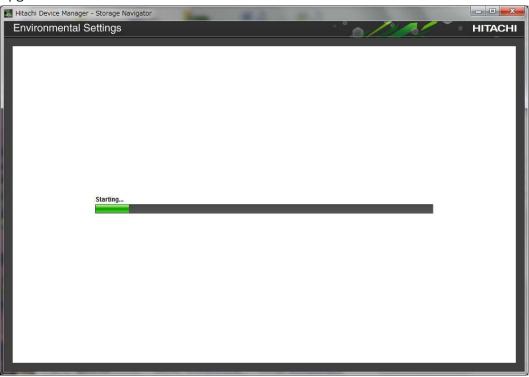
**Note:** The upgrade time can take up to 9 hours to complete when NAS modules are installed.

#### Procedure

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



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



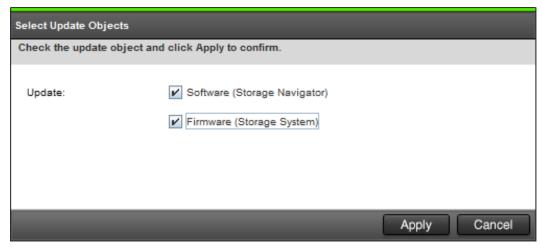
**5.** Wait for the preparation to complete and for the target storage systems list window to open.

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

	er - Storage Navi	igator					
vironmental	Settings		10	HITAC			
ie case of adding the storage system, push [add] button. ie case of changing the target of update, select the storage systems and push [Select Setup Object] button.							
he case of editing the	setting of the storage	e system, select the st	orage system and push [Edit] button. Push [Apply] button t	for executing setup.			
				Refresh			
Storage Syste	ms						
Select All							
System Name	Туре	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)			
unit0	VSP G800	300001	83-01-03-60/00 -> 83-01-20-60/02	83-01-20-60/00 -> 83-01-20-60/02			
Add Selec	t Update Objects	Edit Re	move	Selected: 1 of 1			

The Select Update Objects window opens.

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



8. Click Apply.

The **Update software and firmware** window opens.

9. Click Confirm.

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

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

The software update in progress. Push [Update] button for starting the firmware update. All software and firmware are updated, push [Close] button for exit the Environmental Settings. System Name Type Serial Number Software (Storage Navigator) Firmware (Storage System)	IITACHI
Push [Update] button for starting the firmware update.         All software and firmware are update.         System Name         Type       Serial Number         Software (Storage Navigator)         Firmware (Storage System)	
Push [Update] button for starting the firmware update.         All software and firmware are updated, push [Close] button for exit the Environmental Settings.         System Name       Type         System Name       Type         Serial Number       Software (Storage Navigator)         Firmware (Storage System)	
System Name Type Serial Number Software (Storage Navigator) Firmware (Storage System)	
Storage1 VSP 0800 400102 🕑 Inprogress 36 (Select Update) Update	
	Close

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

<text></text>	she I	litachi Device Manager	- Storage Navigate	or -					_ 🗆 🗙
The software update in progress.         Ash Durbang buttom for starting the firmware update.         As othware and firmware are updated, push (Close) buttom for exit the Environmental Settings.         System Name       Type         Serial Numbar       Software Nonce         Starting the firmware (Storage System)         Storage1       Usp 6800         Horizet       Improgress         Storage1       Usp 6800	E	Environmental S	Settings						• HITACHI
Al software and firmware are updated, push (Close) button for exit the Environmental Settings.									
Storage1       VSP 0600       400102       Inprogress       (Salect Update)       Update		The software update in pro Push [Update] button for sta All software and firmware a	gress. arting the firmware u are updated, push [C	pdate. lose] button for exit t	he Environment	al Settings.			
Storage1       VSP 0600       400102       Inprogress       (Salect Update)       Update			_				_		
								irmware (Storage S	
		Storage1	VSP 6800	400102	Inprogress		(Select Update)		Opdate
Close									
Close									
Cicce									
Close									
Cicse									
Cicse									
Close									
Cicse									
Close									
Close									
Close									
Close									
Close									
Close									
Close									
Close									
									Close

#### Note:

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

If the message displays, use the following corrective action:

- a. Open the **Update Firmware** window from the newly opened **Maintenance Utility** window.
- **b.** Verify the **Update Firmware** window is displaying. If the progress window appears, the firmware is currently updating. Wait until the firmware update is complete.
- **c.** Perform the Force Release System Lock.

The following table shows the possible status conditions.

Status	Description
Waiting	Software waiting to be upgraded. Software components are upgraded individually.
In progress	Software is running.
Completed	Software upgrade is complete.
Failed	Software upgrade failed. Click <b>Update</b> to display the <b>Update Firmware</b> window and review the error details.
Communication Timeout	The completion of the firmware update in time ¹ is not confirmed. Verify the state in the <b>Update</b> <b>Firmware</b> window.
(Not Update)	Not selected as a firmware upgrade target.
Note:	•

1. When NAS Modules are not installed, the installation time is approximately 3.5 hours. When NAS modules are installed, the installation time is approximately 9 hours.

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

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

12. When the following window opens, click Update.

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

	litachi Device Manager		r			_ 🗆 ×
E	Environmental S	Settings				HITACHI
	The software update in pro Push [Update] button for st	arting the firmware up	odate.			
	All software and firmware	are updated, push [Cl	ose] button for exit th	e Environmental Settings.		
	System Name	Туре	Serial Number	Software (Storage Navigator)	Firmware (Storage System	
	🇊 Storage1	VSP G800	400102	Dinprogress 2%	(Select Update) Up	odate
						Close

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

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

🍝 Maintenance Util	ity		- • <b>×</b>
Update Firmw	/are		
	In Progress Upload files : 14 % 9437440 . Update firmware : 0 %	/ 67109120 Bytes	
Firmware	Firmware Detail	Approx.	Status
GUM	-	90 min	Uploading

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

Description
Click <b>Update</b> to display the <b>Update</b> <b>Firmware</b> window.
The <b>Update Firmware</b> window started and the firmware upgrade is not complete. This status appears even if the firmware upgrade is canceled.
Firmware upgrade is complete.
Firmware upgrade failed. Click <b>Update</b> to display the <b>Update Firmware</b> window and review the error details.
The time ¹ required to complete the firmware upgrade cannot be confirmed. Verify the state in the <b>Update</b> <b>Firmware</b> window.
Not selected as a firmware upgrade target.

#### Note:

1. When NAS Modules are not installed, the installation time is approximately 3.5 hours. When NAS modules are installed, the installation time is approximately 9 hours.

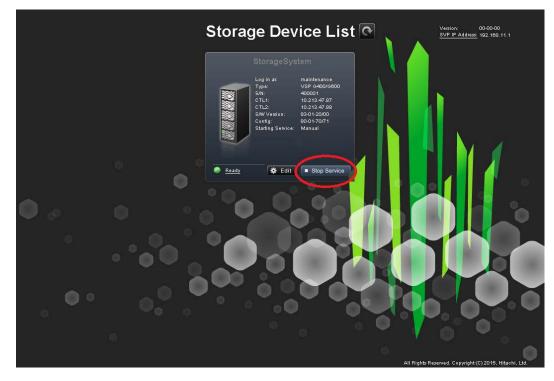
- **16.** In the **Environmental Settings** window, click **Close**.
- **17.** At the **Confirm exit** window, click **Confirm**.

#### Stopping the SVP service

Before upgrading the SVP software, stop the SVP service.

#### Procedure

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



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



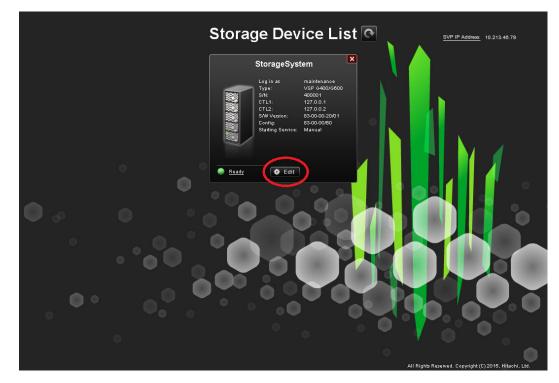
6. Proceed to <u>Upgrading the software (on page 190)</u>.

### Upgrading the SVP software using Storage Device List

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

#### Procedure

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



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

Software:			
Software Selection:			Browse
10.000	_		
Connect Information: IP Address (CTL1):	IPv4	Q IPv6	
IP Address (CTL2):	(i) IPv4	O IPv6	
	( Maoc, 180 oha	aracters)	
System Name:	( Maoc, 180 oha	macters )	
Description:			
Description:	( Max, 180 cha	aracters, or blank )	
Description:	(Mao, 180 cha	aracters, or blank )	
20	( Maoc, 180 oha	aracters, or blank )	
User Information:	( Max, 180 cha ( Max, 256 cha		
User Information:			
User Information: User Name:		aracters)	

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



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

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

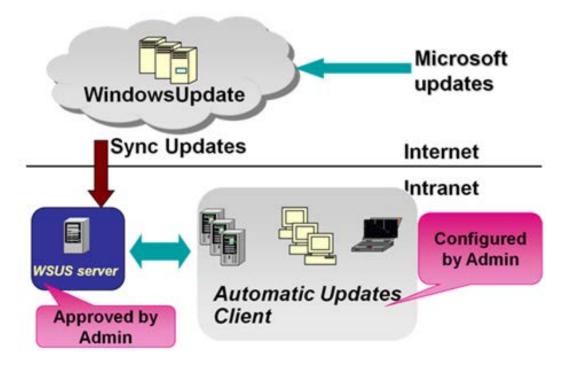
## Downgrading the SVP software

Before downgrading the SVP software, contact the customer support.

# Chapter 10: Security patch and antivirus software

Hitachi Vantara provides a list of suggested antivirus software applications for the SVP. Administrators perform the necessary security measures by applying antivirus software, Windows updates, and security patches according to their internal security policies.

Users apply security patches using a Windows Server Update Services server. Users can also apply security patches using a Windows Server Update Services server.



For the latest antivirus details, see the *SVP* (*Service Processor*) *OS* and *Hypervisor support* for *Gx00*, *Fx00* report at <u>https://support.hitachivantara.com/en_us/interoperability.html</u>.

## **Online update**

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

Chapter 10: Security patch and antivirus software

Change settings		
🜀 🕦 - Control Panel - Al Control Panel Items - Windows Update - Change settings	✓ GD Search Control	
Closes for Windows can install updates         When your compare is only. Windows can instantiately check for inportant op the observation of the observation of the observation of the observation of the result in data windows         Interface       Interface         Int	Monute computer.	polection Control Parel Device and Protes Control Parel Device and Protes Deficit Programs Adventrative Tools High and Support Run
	4 Back	Windows Security
	Search programs and files	Log off 🔸

## **Offline update**

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

Windows 7	HTTP:// WWW.MICROSOFT. COM/EN-US/ SEARCH/ DOWNLOADRESUL TS.ASPX? Q=WINDOWS +EMBEDDED +STANDARD +7&FIRST=11	HTTP:// WWW.MICROSOFT.CO M/EN-US/ DOWNLOAD/ DETAILS.ASPX? ID=41269	
Windows 10 Professional and Windows 10 Enterprise	https://support.micr 4000825/windows-10	osoft.com/en-us/help/ 0-update-history	
Windows Server 2012	https://www.microsoft.com/en-us/ download/details.aspx?id=35626		

## Installing antivirus software on the SVP

Installing antivirus software might affect SVP performance. Therefore, install antivirus software according to the following procedure.

Chapter 10: Security patch and antivirus software

For the latest antivirus details, see the *SVP* (*Service Processor*) *OS* and *Hypervisor* support for *Gx00*, *Fx00* report at <u>https://support.hitachivantara.com/en_us/interoperability.html</u>.

When you install antivirus software on the SVP, observe the following guidelines:

- 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 Device Manager - Storage Navigator. Doing so 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.

#### Procedure

- 1. Log on to the SVP.
- **2.** Install the antivirus software. If the SVP restarts, log on to the SVP again. If the SVP does not restart, restart the SVP manually, and then log on to it .
- **3.** Open the maintenance utility window and verify that there is no failure.

## **Chapter 11: Setting up SSL encryption**

You can set up a Secure Sockets Layer (SSL) connection between the storage system and the SVP.

SSL encrypts 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.

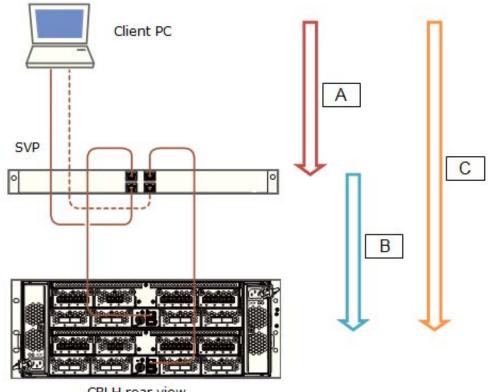
The following terms are associated with SSL:

- 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
В	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"
С	Between the client PC and storage system	Operation of maintenance utility	The certificate for "Web server"



**CBLH** rear view

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

Ë

- 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

- 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

Chapter 11: Setting up SSL encryption

Service Processor Technical Reference

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 reg -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

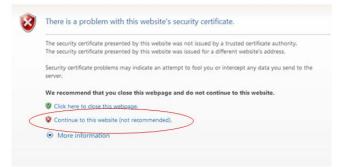
- 1. On the SVP, start a Windows command prompt as Administrator.
- 2. Move the current directory to the directory where the certificate update tool (MappSn2GumSslCrtInit.bat) is located. Issue the following command: C:\MAPP \wk\Supervisor\MappIniSet\MappSn2GumSslCrtInit.bat

**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.

#### Before you begin

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

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

#### Procedure

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

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

The Maintenance Utility logon window opens.

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

Chapter 12: Changing the storage IP address

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

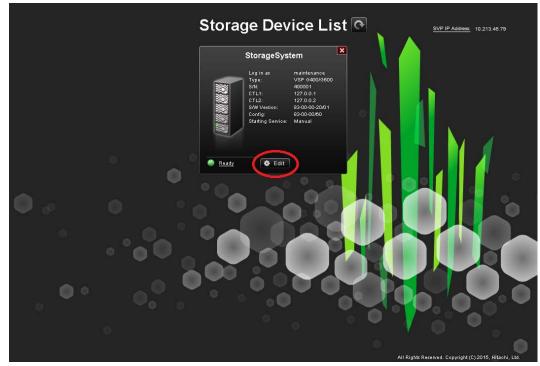


**Note:** If you encounter a problem, troubleshoot the spanning tree protocol.

## Changing storage system information in the Storage Device List

#### Procedure

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



The **Edit System** window opens.

Edit System				
Set values for the new System and click Apply to confirm.				
Software: Software Selection:		Browse		
System Selection:	Auto Discovery     Manual			
Connect Information:				
IP Address (CTL1):	IPv4     IPv8     I0.213.75.134			
IP Address (CTL2):	IPv4 IPv6 10.213.75.136			
System Information:				
System Name:	unit0 ( Max, 180 characters )			
Description:				
	(Max, 180 characters, or blank)			
User Information:				
User Name:	maintenance ( Max, 256 characters )			
Password:	(Max, 256 characters )			
Start service automatically, when the SVP is rebooted.				
	Apply	Cancel		

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 12: Changing the storage IP address

## **Chapter 13: Changing the SVP IP address**

You can change the IP address for the SVP using the Windows 7 or 10 operating system on the SVP or the Storage Device List.

## **Changing the SVP IP address in Windows 7**

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.

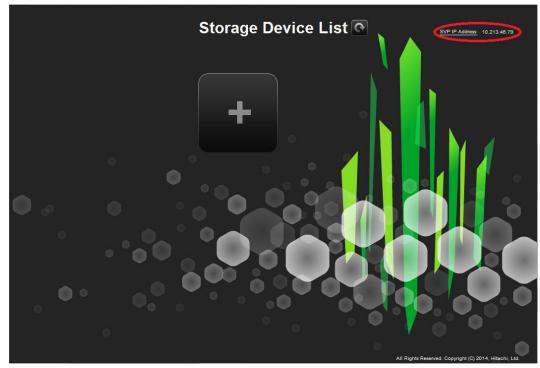
#### Before you begin

- Do not register the storage system on the SVP.
- Do not start the start the storage system service.

#### Procedure

- 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.

Chapter 13: Changing the SVP IP address



The Change SVP IP Address window opens.

Change SVP IP Address				
Set IP address for the SVP and click Apply to confirm.				
and ener Apply to commit.				
	3			
10.231.98.137				
	Apply	Cancel		

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

Chapter 13: Changing the SVP IP address

# Chapter 14: Changing and initializing SVP port numbers

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

## **Changing SVP port numbers**

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

#### Before you begin

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

#### Procedure

- 1. Request all users to log out of Device Manager Storage Navigator.
- 2. On the SVP, exit to a Windows command prompt as Administrator.
- 3. Change to the directory to the location of the tool MappSetPortEdit.bat.
- 4. Enter the following command: C:\Mapp\wk\Supervisor\MappIniSet
  \MappSetPortEdit.bat _ [port number key name] _ [port number]
  where _ indicates a space and the values [] indicate a parameter. For example:
  >cd C:\Mapp\wk\Supervisor\MappIniset\mappsetportedit.bat
  MAPPWebServer 10001
  - **Note:** In this command, C:\MAPP indicates the installation directory of the storage management software and SVP software. If the installation directory is not C:\Mapp, replace C:\Mapp with the appropriate installation directory.

Chapter 14: Changing and initializing SVP port numbers

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
MAPPWebServ er	HTTP	80	Yes	83-01-20- xx/00 or later
MAPPWebServ erHttps	HTTPS	443	No	
RMIClassLoad er	RMI	51099	No	
RMIClassLoad erHttps	RMI (SSL)	5443	No	
RMIIFRegist	RMI	1099	No	
PreRMIServer	RMI	51100-51355 ¹	No	
		Automatic allocation		83-03-01- xx/00 or later
DKCManPrivat e	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	83-01-20- xx/00 or later
		Automatic allocation	used.	83-03-01- xx/00 or later
CommonJettyS tart	НТТР	8080	N/A	83-01-24- xx/00 or later
CommonJettyS top	HTTP	8210	N/A	
RestAPIServer Stop	HTTP	9210	N/A	

Chapter 14: Changing and initializing SVP port numbers

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

#### Note:

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

Chapter 14: Changing and initializing SVP port numbers

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 <u>Viewing the port number to</u> be used in the SVP (on page 225).
- 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 <u>Initializing</u> <u>automatically allocated port numbers (on page 222)</u>.

#### **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="">.</svp>
MAPPWebServerHttps	<b>Using Hitachi Device Manager - Storage</b> <b>Navigator</b> : None
	Using Hitachi Command Suite
	Match the port number used in Hitachi Command Suite to <svp change="" port="">.</svp>
RMIClassLoader	None
RMIClassLoader	Using Hitachi Command Suite
	Match the port number used in Hitachi Command Suite to <svp change="" port="">.</svp>

RMIClassLoaderHttps	Using <b>Hitachi Device Manager - Storage</b> 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.</svp>
RMIIFRegist	When issuing the remote power ON/OFF tool (RmtPsTool) command, specify <svp Change Port&gt; for the Management Server Port Number parameter.</svp 
	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.</svp>
	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="">.</svp>
SMIS_CIMOM	Match the port number used in the SMI-S communication to <svp change="" port="">.</svp>
	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 <u>Viewing the port number to be used in the SVP (on page 225)</u> )
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 <u>Reallocating</u> <u>automatically allocated port numbers (on page 221)</u>.

#### Procedure

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

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

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

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

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

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

**12.** Start the service of the storage system.

# Changing range of port numbers to be allocated automatically

## Before you begin

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

#### Procedure

- 1. On the SVP, start a Windows command prompt as an Administrator.
- 2. Change the current directory to the directory where the tool exists and run the following command: C:\Mapp\wk\Supervisor \MappIniSet>MappPortRangeSet.batr[Service port number]_[Range of port numbers]
  - **Tip:** C:\MAPP indicates the installation directory of the storage management software and SVP software. If the installation directory is not C:\Mapp, replace C:\Mapp with the appropriate installation directory.

## Note:

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

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

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

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

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

 You can specify more than one command input parameter "[Service port number key name] * [Port number range] where * is a one-byte space.

For example, MappPortRangeSet.bat PreRMIServer 51200-55000 SMIS_CIMOM 5989-6244,8000

• The port number range set for unavailable cannot be used, even if it is an effective range for other keys.

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

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

# Initializing range of port numbers to be allocated automatically

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

## Before you begin

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

## Procedure

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

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

**3.** The confirmation message for reallocation is displayed. To continue the processing, enter y, and then press **Enter**. To cancel the processing, enter n, and then press **Enter**.

A completion message appears. Press any key to continue.

**4.** Close the command prompt.

## Viewing the port number to be used in the SVP

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

## Before you begin

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

## Procedure

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

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

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

- **Tip:** C: \MAPP indicates the installation directory of the storage management software and SVP software. If the installation directory is not C: \Mapp, replace C: \Mapp with the appropriate installation directory.
- **3.** The information of the port numbers to be used in the SVP is displayed. For the ports whose numbers are not allocated, **Not Defined** is displayed.
- **4.** A completion message appears. Press any key to continue.
- **5.** Close the command prompt.

## **Chapter 15: Editing the Storage Device List**

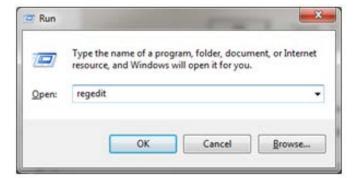
If you change the storage system IP address or the maintenance password, edit the Storage Device List to reflect the change.

#### Procedure

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



- 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.



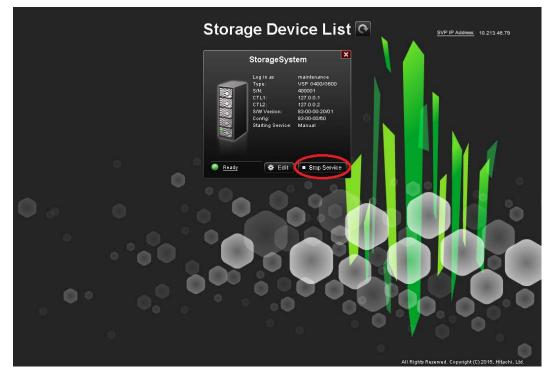
- e. Go to the following key: HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\BridgeMP
- f. Right-click New > DWORD (32-bit Value), and then type DisableSTA.

Ele Edit View Favorites BridgeMP		Name		Data
	-		Туре	1
Browser	-131	(Default)	REG_SZ	(value not set)
Brserid		ab Device	REG_SZ	¥Device¥{D940C8D7-84CD-42A8-9580-4F16B92C5302
BrSerWdm		118 DisableSTA	REG_DWORD	0x00000001(1)
BrUsbMdm		ab DisplayName	REG_SZ	@%SystemRoot%¥system32¥bridgeres.dl,-1
BrUsbSer	1018	# ErrorControl	REG_DWORD	0x00000001 (1)
BTHMODEM BTHPORT	1	ab Group	REG_SZ	PNP_TDI
		ab ImagePath	REG EXPAND SZ	system32#DRIVERS#bridge.sys
bthserv		116 Start	REG_DWORD	0x00000003 (3)
cdfs cdrom		11 Tag	REG_DWORD	0x0000000a (10)
CertPropSvc		118 Type	REG_DWORD	0x00000001(1)

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

Edit DWORD (32-bit)	Value X
Value <u>n</u> ame:	
DisableSTA	
⊻alue data: ∎	Base <u>H</u> exadecimal <u>D</u> ecimal
	OK Cancel

- 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.

-66	e http://19	92.168.0.17/			-
Favorites	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	uggested Sites 🔻	🟉 Web Slice	Gallery -	

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

Maintenance Ut	ility			Alert System Unit	ocked Logged in as: maintenance Log Out ?
Storage System		Network Settings			Last Updated : 2015/09/16 18:16 🔯
	Ready	Set Up Network Settings	Set Up Network Permissions		
Serial Number	407001			CTL1	CTL2
	: CTL2	IPv4 Configuration	IPv4 Address	10.213.74.111	10.213.74.112
			Subnet Mask	255.255.255.0	255.255.255.0
	limute		Default Gateway	10.213.1.1	10.213.1.1
Administration			DNS Server 1	10.213.1.2	10.213.1.2
Talinord			DNS Server 2	10.213.1.3	10.213.1.3
Alert Notifications			DNS Server 3		
Concertbeb		IPv6 Configuration	IPv6 Address		
Network Settings		and the second process of	Link Local Address		· · · · · · · · · · · · · · · · · · ·
Dare Lettant			Subnet Prefix Length		
			Default Gateway		
ក្រុ Audit Log Settings			DNS Server 1		
			DNS Server 2		
			DNS Server 3		•
		MAC Address		XX+XX+XX+XX+XX+XX+XX	30(+)(X+30(+)(X+30(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(X+30)(+)(
		Network Connection Mod	e	10Mbps HALF	100Mbps FULL
		Maintenance Port		192.168.233.116	192.168.233.117

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

ternet Protocol Version 4 (TCP/I	Pv4) Prope	rties	
Seneral			
You can get IP settings assigned au this capability. Otherwise, you need for the appropriate IP settings.	to ask your n		
C Obtain an IP address automation — • Use the following IP address:	cally		
IP address:	10 . 4	. 9	, 42
Subnet mask:	255 .25	5 .255	. 128
Default gateway:	10 . 4	, 9	, 126
C Obtain DNS server address au C Use the following DNS server a Preferred DNS server: Alternate DNS server:	ddresses:	70 1.	

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



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

Set IP address and click App			
IPv4			
10.4.9.42			
-	1	Apply	Cancel

**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**.

Software: Software Selection:	Erowse
System Selection:	Auto Discovery     O Manual
Connect Information:	
IP Address (CTL1):	IPv4  IPv6
	10.4.9.43
IP Address (CTL2):	IPv4 O IPv6
	10.4.9.44
Description:	MODEL H / 0800
	(Max, 180 characters, or blank)
User Information:	
User Name:	maintenance
	( Max, 256 characters )
Password:	

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

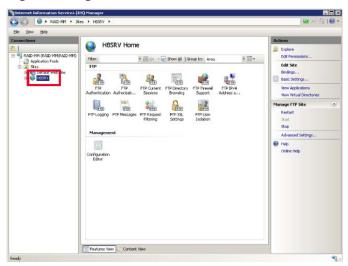


- **14.** Using Remote Desktop Connection, access the SVP using the new user LAN IP address.
- **15.** Open the **Storage Device List** window and verify that services are ready.

Chapter 15: Editing the Storage Device List



- **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**.

Chapter 15: Editing the Storage Device List

RAID-MM + Sk							90 - B
Dev Delp						A	tions
	Sibes						Add Web Ste
RAID-MM (RAID-MM(RAID-MM)	fike:			Group by: No Grouping	+		Set Web Site Defaults
Add Web Ste	efault Web Ste	10	Status Stopped (N	6inding	Path %St		Set FTP Ste Defeute
Pin Dafrach						0	l Help
Add FTP Site							Online Help
Switch to Contern Her							
						L	
	4						

d. For FTP site name, type H8SRV. For Content Directory, type C:\Mapp\wk \83xxxxyyyyy\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

Site Information		?
TP site name:	٦	
Content Directory		
Physical path:		

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

Binding IP Address:	Por		
All Unassigned		<u>.                                    </u>	
Enable Virtual Host Names:			
Virtual Host (example: ftp.co	ontoso.com):		
Conternation to the state			
Start FTP site automatically			
SSL			
Start FTP site automatically SSL No SSL			
SSL No SSL Allow SSL			
SSL No <u>S</u> SL			

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

Authe	ntication a	nd Authorization	Information	?
Authentication				
Resic				
Authorization Allow access to: All users	1			
Permissions	-			
I▼ Rea <u>d</u> I▼ <u>W</u> rite				

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

Windows Pirewall with Advanced S	Inbound itules						Actions	-
Inhound Rules	Name	Group	Profile	Enabled	Action	1.	Inhound Rules	
Connection Security Pulses	Ple and Printer Sharing (Scho Request - JCM	Pile and Printer Sharing	Public	Yes	Alow		1 New Rule	
Monitoring	File and Printer Sharing (Echo Request - ICM	File and Printer Sharing	Private	No	Alow		The second secon	
and constrainty	Pile and Printer Sharing (Echo Request - ICM	Pile and Printer Sharing	Domein	Yes:	Alow		Y Fiber by Profile	2
	The and Printer Sharing (Scho Request - SCM		Public	Yes	Alow		V Filter by State	- 9
	File and Printer Sharing (Echo Request - ICM		Domain	Ves	Allow		ST Filter by Group	5
	Pile and Printer Sharing (Scho Request - )CM		Private	No	Alow		A 1404 01 000	12
	The and frinter Sharing (LIMMR-UDF-(n)	File and Printer Sharing	Domai		Alow		View	-0
	File and Printer Sharing (LUMIR-LIDP-In)	File and Printer Sharing	Public	Ves	Alow		G Refresh	
	File and Printer Sharing (VE-Datagram-In)	File and Printer Sharing	Public	Vec	Alow		CX remen	
	File and Printer Sharing (NE-Dalagram-In)	File and Printer Sharing	Domein	No	Alow		Export List	
	File and Printer Sharing (NB-Datagram-3n)	File and Printer Sharing	Private	No	Allow		R Heb	
	Giffle and Printer Sharing (Nb-Naire-In)	File and Printer Sharing	Public .	Yes	Alow	0	1.00	
	File and Printer Sharing (MD-Name-In)	File and Printer Sharing	Privabe	No	Alow		Selected Items	10
	File and Printer Sharing (NE-Name-In)	File and Printer Sharing	Domain	No	Alow		C Enable Pale	-
	File and Printer Sharing (ND-Session-In)	File and Printer Sharing	Public	Ves	Allow			
	Pile and Printer Sharing (VB-Session-3n)	File and Printer Sharing	Private	No	Alow		a cut	
	The and Protor sharing (V& Seison-3h)	Pile and Printer Sharing	Domain	No	Alow	-	Copy	
	File and Frister Sharing (SNE-Iz)	File and Printer Sharing	Private	No	Alow			
	Pile and Printer Sharing (SMI-In)	Pile and Printer Sharing	Domein	No	Alow		X Delete	
	Cific and Printer Sharing (SMD In)	File and Printer Sharing	Public	Ves	Alow		17 Help	
	File and Printer Sharing (Sposler Service - RPC)		Public	Ves	Alov			
	This and Printer Sharing (Sposler Service - RPC)		Domein	No	Alov			
	File and Phinter Sharing (Sposler Service - RPC)		Privaba	No	Allow			
	File and Printer Sharing (Sposler Service - R		Domein	No	Alow			
	The and Proter Sharing (Sposler Service - R		Public	Yes	Alow			
	File and Printer Sharing (Sposler Service - R		Privabe	No	Allow			
	Whetworking - Echo Request (ICMPv4-In)	File and Printer Sharing	Public	Ves	Alow			
	Whetworking - Echo Request (ICMPvt-In)	Pile and Printer Sharing	Public.	Ves	Alow	- 11	1	
	FIP Server (FIE InaMin Ini	FIP Server	45	NE	Allow		1	
	TP Server Possive (FTP Page removed and TTP Server Secure (FTP St) _ Enable Fulle		All	N	Alow		1	
	Character and Ch		Privata	No	Allow	- 11	1	
	Contemporaria (Charles)	wiroup	Private	No	Alow		1	
	CODY Courses (TCR. In)	ST Service	Domain	No	Allow		1	
	Griscal Service (TCP-In) Delete	2 Service	Privat	No	Alow		1	
	Rev Panagement Service (TCP-	Management Service	Privat		Alow		1	
	Key Nanagement Service (TCP-in)	Key Management Service	Domain	No	Alow		-	

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 15: Editing the Storage Device List

# Chapter 16: Deleting and registering the storage system

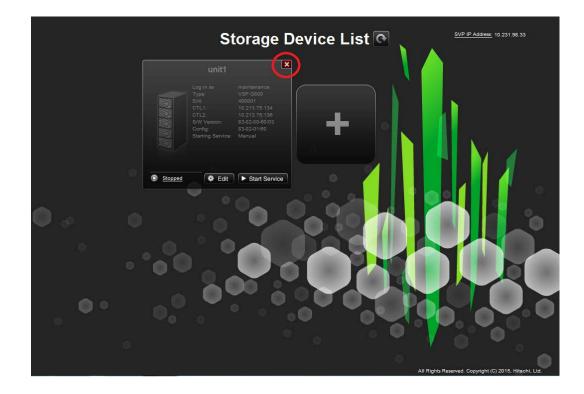
In the unlikely event you need to delete the storage system from the Storage Device List, use the following instructions to delete the storage system, and then register it on the SVP.

# 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 <u>Stopping and restarting the service in each storage system</u> (on page 176)).
- 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

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

## Before you begin

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

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

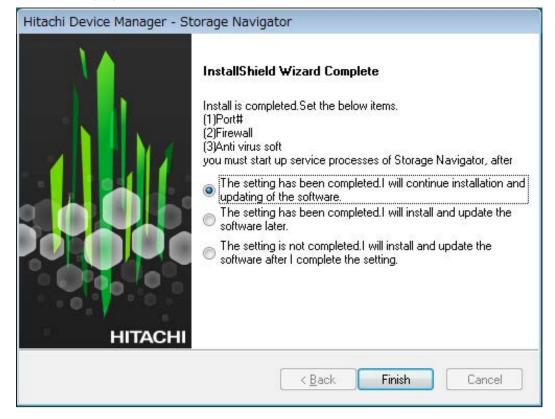
•
-

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

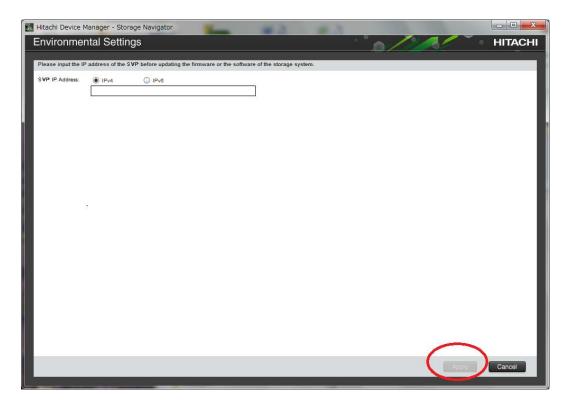
## Procedure

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

- 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.

🛃 Hitachi Device Manager - Storage Navigator	
Environmental Settings	• HITACHI
In the case of adding the storage system, push [Add] button. In the case of changing the target of update, select the storage systems and push [Select Update Object] button.	
In the case of editing the setting of the storage system, select the storage system and push [Edit] button. Push [Apply] button for executing setup.	_
	Refresh
Storage Systems	
Select All	
System Name Type Serial Number Software Version (Storage Navigator) Firmware Version (Storage Navigator)	age System)
Empty	
Add Select Update Objects Edit Remove Sele	cted: 0 of 0
Appl	Cancel

The **Add System** window opens.

Add System	
Set values for the new \$	System and click [Apply] to confirm.
System Selection:	Auto Discovery     Manual
IP Address (CTL1):	IPv4 IPv6
IP Address (CTL2):	● IPv4 ○ IPv6
System Name:	( Max, 180 characters )
Description:	
	( Max, 180 characters, or blank )
User Name:	( Max, 256 characters )
Password:	( Max, 256 characters )
Not start service af	ter addition immediately
	Apply Cancel

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.
	<ul> <li>Auto Discovery: Acquire the storage system information automatically. (default)</li> </ul>
	<ul> <li>Manual: Specify the storage system manually.</li> </ul>

Field	Description
IP Address (CTL 1)	Enter the IP address for controller 1. Accept the default <b>IPv4</b> setting or click <b>IPv6</b> , and then enter the IP address in the appropriate format for the addressing method selected.
IP Address (CTL 2)	Enter the IP address for controller 2. Accept the default <b>IPv4</b> setting or select <b>IPv6</b> , and then click the IP address in the appropriate format for the addressing method selected.
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.

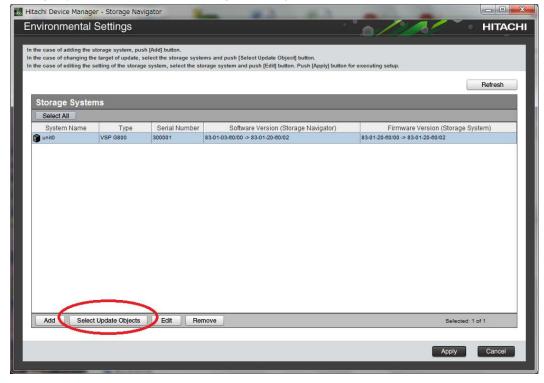
## 9. Click Apply.

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

litachi Device Manage	er - Storage Nav	rigator	#3 #3	
nvironmental :			18	HITACH
n the case of adding the s n the case of changing the			ems and push [Select Update Object] button.	
n the case of editing the s	etting of the storag	e system, select the st	orage system and push [Edit] button. Push [Apply] button	for executing setup.
				Refresh
Storage Syster	ns			
Select All				
System Name	Туре	Serial Number	Software Version (Storage Navigator)	Firmware Version (Storage System)
unit0	VSP G800	300001	83-01-03-60/00	83-01-20-80/00
Add	Update Objects	Edit Rei	nove	Selected: 0 of 1
				Anply Cancel

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

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



The **Select Update Objects** window opens.

Select Update Object	ts	
Check the update of	bject and click Apply to confirm.	
Update:	Software (Storage Navigator)	
	Firmware (Storage System)	
		Apply Cancel

- **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.

Hitachi Device Manager - Storage Navigator						
Environmental	HITACH					
In the case of adding the storage system, push [Add] button. In the case of changing the target of update, select the storage systems and push [Select Update Object] button.						
			orage system and push [Edit] button. Push [Apply] button	for executing setup.		
				Refresh		
	807					
Storage System	ns					
Select All	-					
System Name	Type VSP G800	Serial Number 300001	Software Version (Storage Navigator) 83-01-03-60/00 -> 83-01-20-60/02	Firmware Version (Storage System) 83-01-20-60/00 -> 83-01-20-60/02		
Unito	V3F 0800	300001	83-01-03-00/00 -> 83-01-20-00/02	83-01-20-00/00 -> 83-01-20-00/02		
Add Select	Update Objects	Edit Rei	nove	Selected: 1 of 1		
				Apply Cancel		

**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.

nvironmental	Settings					
e software update in pro sh [Update] button for s software and firmware	tarting the firmware	update. [Close] button for exit ti	he Environment	al Settings.		
System Name	Туре	Serial Number		Software (Storage Navigator)	Firmwa	re (Storage System)
Storage1	VSP G800	400102	🕞 Inprogress	ow.	(Select Update)	Update
						Close

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

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.

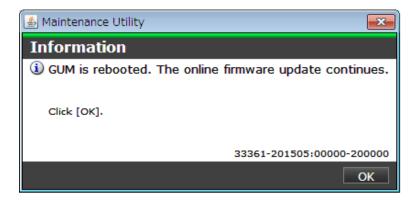
nvironmental	Settings					
e software update in pro ish [Update] button for st I software and firmware	arting the firmware	e update. [Close] button for exit t	he Environment	al Settings.		
System Name	Туре	Serial Number		Software (Storage Navigator)	Firm	ware (Storage System)
Storage1	VSP G800	400102	Inprogress	3%	(Select Update)	Update

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

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

mitre +		adata information				
	n click [Apply	pdate information,				
			is communication d	isconnect done by a G	IM rostart	
when	doing a minim	are renewal, there	is communication u	isconnect done by a G	JM Testart.	
A No.	-					
\rm Noi	mai.					
Jootod	Firmularo Filo: C	WOLIM EWIIDDATE 0190	07 20150204 mda			
elected	Firmware File: C	¥GUM_FWUPDATE_0139	107_20150204.mda			
rmware	Version					
	<b>C</b> .	Firmware Detail	Current Version	New Version	Message	
2						
<b>V</b>	Firmware		Current Version		Message	
V	DKCMAIN	-		83-00-00-20/08	Message	
V V	DKCMAIN FCHF	- -		83-00-00-20/08 83-00-01-10	INIESSABE	
<ul> <li>✓</li> <li>✓</li> </ul>	DKCMAIN			83-00-00-20/08		
V V V	DKCMAIN FCHF			83-00-00-20/08 83-00-01-10		
	DKCMAIN FCHF ISCSI			83-00-00-20/08 83-00-01-10 83-01-01-04		
	DKCMAIN FCHF iSCSI DKB			83-00-00-20/08 83-00-01-10 83-01-01-04 83-07-00		
	DKCMAIN FCHF ISCSI DKB RAMBOOT			83-00-00-20/08 83-00-01-10 83-01-01-04 83-07-00 83-00-05		
	DKCMAIN FCHF ISCSI DKB RAMBOOT Expander			83-00-00-20/08 83-00-01-10 83-01-01-04 83-07-00 83-00-05 90-09-02		
	DKCMAIN FCHF ISCSI DKB RAMBOOT Expander CONFIG	- - - - - - - - - - -		83-00-00-20/08 83-00-01-10 83-01-01-04 83-07-00 83-00-05 90-09-02 83-00-04/00		
	DKCMAIN FCHF ISCSI DKB RAMBOOT Expander CONFIG CFM	- - - - - - - - - - MI1		83-00-00-20/08 83-00-01-10 83-01-01-04 83-07-00 83-00-05 90-09-02 83-00-04/00 01-34-00-00		

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



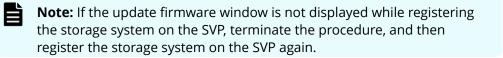
- 18. Click OK.
- **19.** Wait for the firmware upgrade to complete, and then verify the firmware update status in the **Firmware (Storage System)** column of the **Environmental Settings** window. Wait for the firmware update to complete. The following table lists the status conditions.

Description
Click <b>Update</b> to display the <b>Update</b> <b>Firmware</b> window.
The <b>Update Firmware</b> window started and the firmware upgrade is not complete. This status appears even if the firmware upgrade is canceled.
Firmware upgrade is complete.
Firmware upgrade failed. Click <b>Update</b> to display the <b>Update Firmware</b> window, and review the error details.
The time ¹ required to complete the firmware upgrade cannot be confirmed. Verify the state in the <b>Update</b> <b>Firmware</b> window.
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**.



## 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.

Chapter 17: Back up and restore the SVP

- 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

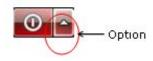
## Procedure

- 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 Vantarasupplied SVP

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

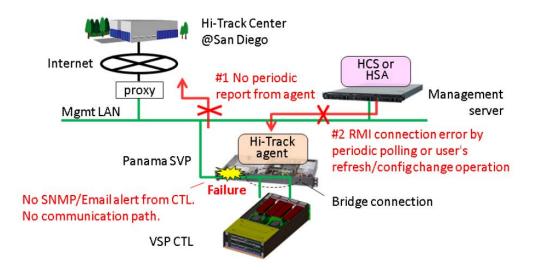
**Important:** The Hitachi Vantara-supplied SVP can only be installed, upgraded, or replaced by a Hitachi Vantara representative or an authorized service provider. Contact a Hitachi Vantara representative for more information about installing, upgrading, or replacing a Hitachi Vantara-supplied SVP.

## **Detecting SVP failures**

SVP failures are detected and resolved using the following methods.

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

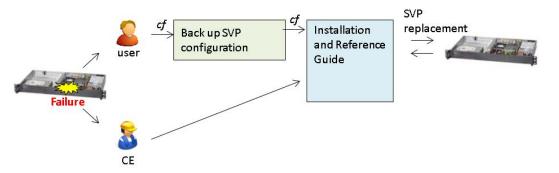
Chapter 19: Replacing the Hitachi Vantara-supplied SVP



## **Replacing the physical SVP**

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

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



## Recovering the operating system

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

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

Chapter 19: Replacing the Hitachi Vantara-supplied SVP

## Backing up the OS

#### Procedure

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

## **Restoring the OS**

#### **Procedure**

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

## Configuring the replacement physical SVP

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

#### Procedure

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

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

## Mapping the internal SVP network adapters

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

#### Procedure

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

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



**5.** Connect an Ethernet cable to the LAN1 port on the SVP. Local Area Connection 7 is assigned to the LAN1 port.



**6.** Remove the Ethernet cable from the LAN1 port and connect it to the LAN2 port on the SVP.

Local Area Connection 6 is assigned to the LAN2 port.



 Repeat step 6 with the LAN3 and LAN4 ports on the SVP. When you connect the Ethernet cable to these ports, Local Area Connection 8 will be assigned to the LAN3 port and Local Area Connection 5 will be assigned to the LAN4 port.

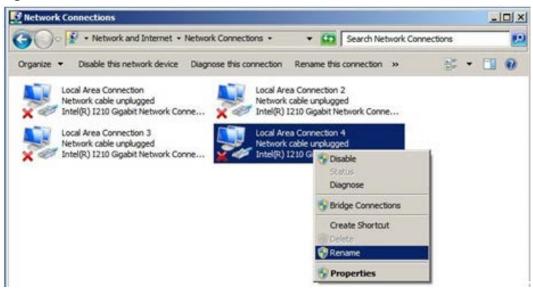


**Note:** Verify that no IP address is configured for the SVP LAN ports. Otherwise, the storage system could become blocked.

Renaming the internal SVP network adapters

#### Procedure

1. Right-click LAN1 (Local Area Connection 4), and then click Rename.



- 2. Change the name to Management (User).
- **3.** Repeat step 1 and step 2 to rename the other three SVP network adapters as follows.

Change the name of this SVP adapter	to this name	Adapter configuration
LAN1	Management(User)	Bridge for the management LAN
LAN2	Maintenance	Maintenance LAN
LAN3	Management(CTL1)	Management LAN
LAN4	Management(CTL2)	Bridge for the management LAN

 Leave the Network Connections window open. Then either configure the SVP for bridge mode or configure the IP addresses for the SVP LAN ports to match the IP addressing scheme of your subnet.

## **Setting the IP address**

After renaming the internal SVP network adapters, perform the initial startup procedures to specify the IP addresses for the SVP and storage system.

#### Procedure

- **1.** Connect a PC to the LAN2 port on the SVP.
- 2. Log on to the SVP using the Remote Desktop Connection:

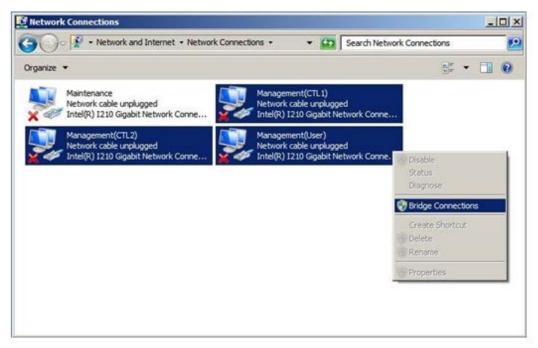
- a. Configure the PC to use an IP address of 10.0.0.xxx, where xxx = 1-99 or 101-254, and a subnet mask of 255.255.255.0.
- b. Click **Start > All Programs**, and then click **Accessories > Remote Desktop Connection**.
- c. In the **Computer** field, type 10.0.100 and click **Connect**.
- d. In the **Windows Security** screen, type SVP-PC\SVP in the top field and raid-login in the bottom field.
- e. Click **OK**.
- f. If prompted that the identity of the remote computer cannot be verified, click **Yes** to continue.
- **3.** In the Remote Desktop Connection window, click **Control Panel** > **Network and Sharing Center**.
- 4. Click Change adapter settings.
- 5. In the **Network Connections** window, right-click the **Management(CTL1)** network adapter, which corresponds to SVP physical port LAN3, and click **Properties**.
- 6. In the Local Area Connection Properties window, double-click Internet Protocol version 4 (TCP/IPv4) or Internet Protocol version 6 (TCP/IPv6), depending on the IP addressing schemes used on your subnet.
- 7. In the dialog box, click **Use the following IP address**.
- **8.** Enter the IP address, subnet mask, and gateway settings in the appropriate fields, and then click **OK**.
- 9. Click OK to close the Local Area Connection Properties window.
- In the Network Connections window, right-click the Management(CTL2) network adapter, which corresponds to the LAN4 port on the physical SVP, and click Properties. Then repeat steps 3 through 7 to assign the TCP/IP settings for this network adapter.
- **11.** Close the **Network connections** window.

## **Configuring bridge settings**

If your environment requires the SVP to operate in bridge mode, you can configure the SVP to operate in bridge mode after you rename the four internal SVP network adapters. In this mode, SVP ports LAN3 and LAN4 connect to the LAN management port on each controller.

#### Procedure

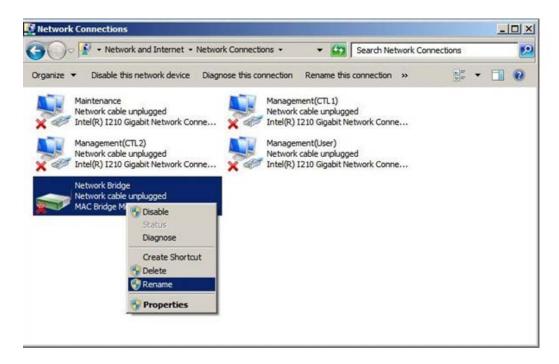
- 1. In the **Network Connections** window, click the LAN1 adapter, and then hold down the Ctrl key and click the LAN3 and LAN4 network adapters.
- 2. Right-click the mouse and click **Bridge Connections**.



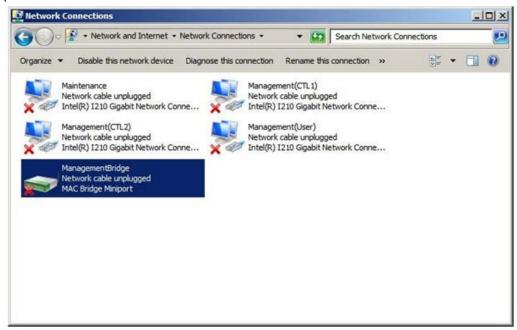
A new instance of Network Bridge appears.



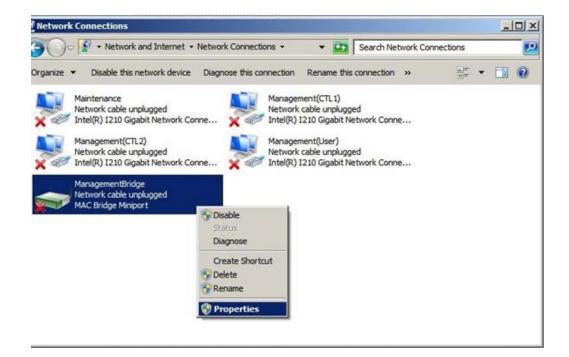
3. Right-click the Network Bridge icon, and then click Rename.



4. Change the name to ManagementBridge. Type this name as one word, with no spaces.



5. Right-click the ManagementBridge icon, and then click Properties.



6. Click Internet ProtocolVersion 4 (TCP/IPv4).

Ketwork Connections		_ 0 ×
🗿 🕞 🔹 Network and Internet	Network Connections      Search Network	Connections 🗾 😥
Organize 👻 Disable this network devic	e Diagnose this connection Rename this connection »	er 🕶 🖬 🔞
Maintenance Network cable unplugged Intel(R) I210 Gigabit Network Network cable unplugged Intel(R) I210 Gigabit Network ManagementBridge Network cable unplugged MAC Bridge Miniport	Management(CTL 1) Network cable unblond         ImagementBridge Properties         Networking         Adapters:         Select the adapters you want to use to connect to compute on your local network.         Imagement(User)         Imagement(User)         Imagement(CTL 1)         Imagement for Microsoft Networks         Imagement for Microsoft Networks	

- 7. Configure the following IP settings for ManagementBridge:
  - IP address : 192.168.0.15 (default)
  - Subnet mask: 255.255.255.0

Network Connections					_101
🌀 🕞 🖓 🔹 Network and Internet	<ul> <li>Network Connection</li> </ul>	ns • •	Search Netw	ork Connections	
Organize  Disable this network device Maintenance Network cable unplugged Intel(R) I210 Gigabit Network		Management(CT Network cable u	nolugged	* <u>*</u> *	• 🖬 🧕
Management(CTL2) Network cable unplugged Intel(R) I210 Gigabit Network	General   You can get this capabilit for the appro	IP settings assig y. Otherwise, yo opriate IP setting an IP address a e following IP ad s: ask:	dress:	our network supp	
	Preferred		ress automatically server addresses:	· · ·	
	— 🗖 Valida	te settings upon	exit	Advance	d
				ок с	ancel

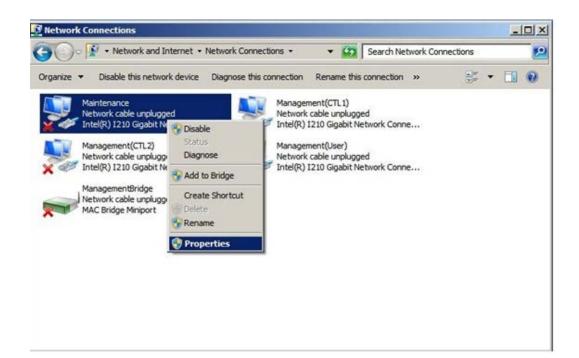
8. Click Advanced, and then click the WINS tab.

0		
ganize      Disable this network device	e Diagnose this connection Rename this connection >>	9÷ • 🖬
Maintenance Network cable unplugged Intel(R) 1210 Gigabit Network Management(CTL2) Network cable unplugged Intel(R) 1210 Gigabit Network ManagementBridge Network cable unplugged MAC Bridge Miniport	Management(CTL1) Network cable undunned ManagementBridge Properties Networking Internet Protocol Version 4 (100/10/4) Properties Advanced TCP/IP Settings IP Settings DNS WINS WINS addresses, in order of use:	
	If LMHOSTS lookup is enabled, it applies to all conn TCP/IP is enabled.	Remove ections for which Import LMHOSTS
	NetBIOS setting     O Default:     Use NetBIOS setting from the DHCP server.     is used or the DHCP server does not provid     enable NetBIOS over TCP/IP.     C Enable NetBIOS over TCP/IP     C Disable NetBIOS over TCP/IP	

9. Under NetBIOS setting, click Disable NetBIOS over TCP/IP, and then click OK.

0,		
anize      Disable this network devi	ice Diagnose this connection Rename this connection »	- 🛄
Maintenance Network cable unplugged Intel(R) I210 Gigabit Network Management(CTL2) Network cable unplugged Intel(R) I210 Gigabit Network ManagementBridge Network cable unplugged MAC Bridge Miniport	Management(CTL 1) Network cable unplanced  Metworking  Internet Protocol Version 4 (TCP/IPv4) Properties  Advanced TCP/IP Settings  IP Settings   DNS   WINS    WINS addresses, in order of use:	?(x) ?))
	I     Add     Edt     Remove       If LMHOSTS lookup is enabled, it applies to all connections for whit TCP/IP is enabled.     Import LMHOSTS       I     Import LMHOSTS     Import LMHOSTS	а.  2
	NetBIOS setting     Oefault:     Use NetBIOS setting from the DHCP server. If static IP ad     is used or the DHCP server does not provide NetBIOS sett     enable NetBIOS over TCP/IP.     Enable NetBIOS over TCP/IP     Disable NetBIOS over TCP/IP	

**10.** Right-click the **Maintenance** icon (LAN2), and then click **Properties**.



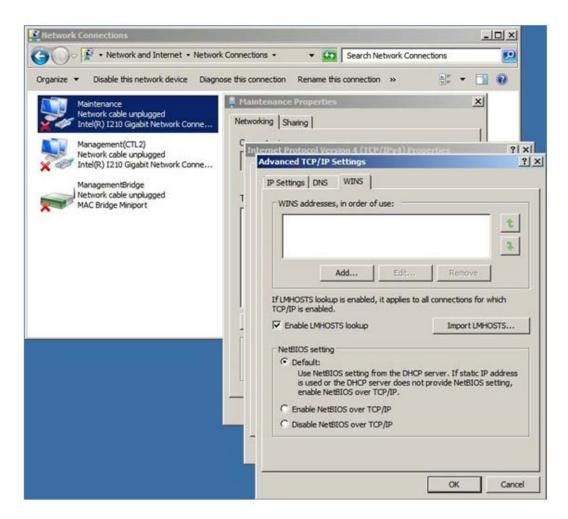
11. Click Internet ProtocolVersion 4 (TCP/IPv4).

Organize   Disable this network device Diagno	se this connection Rename this connection »	-
Maintenance Network cable unplugged Intel(R) I210 Gigabit Network Conne           Management(CTL2) Network cable unplugged Intel(R) I210 Gigabit Network Conne           ManagementBridge Network cable unplugged MAC Bridge Miniport	Maintenance Properties         Networking       Sharing         Connect using:       Connect using:         Intel(R) 1210 Gigabit Network Connection       Configure         This connection uses the following items:       Configure         Otent for Microsoft Networks       Sharing for Microsoft Networks         Gos Packet Scheduler       Link-Layer Topology Discovery Mapper I/O Driver         Link-Layer Topology Discovery Responder       Hetemet Protocol Version 6 (TCP/IPv6)         Hetemet Protocol Version 6 (TCP/IPv6)       Install         Uninstel       Properties         Description       Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse inferconnected networks.	

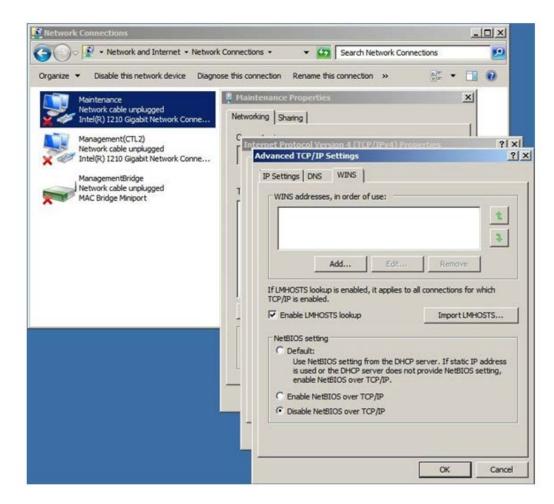
- 12. Configure the following IP settings for Maintenance (LAN2):
  - IP address : 10.0.0.100 (default)
  - Subnet mask: 255.255.255.0

O V Network and Internet	Network Connections	Search Network Connections	
Organize 👻 Disable this network devic	e Diagnose this connection Renam	me this connection »	• 🔟 🔞
Maintenance Network cable unplugged Intel(R) I210 Gigabit Network Network cable unplugged Intel(R) I210 Gigabit Network ManagementBridge Network cable unplugged MAC Bridge Miniport	this capability. Otherwise, yo for the appropriate IP setting C Obtain an IP address au C Use the following IP add I IP address: Subnet mask: Default gateway:	Indunned	
	C Obtain DNS server addr		
	Preferred DNS server:		
	Alternate DNS server:	A A A	
		exit Advanced	

**13.** Click **Advanced**, and then click the **WINS** tab.



14. Under NetBIOS setting, click Disable NetBIOS over TCP/IP, and then click OK.



- **15.** Click **OK** to apply the settings and close the **Local Area Connection Properties** window.
- **16.** Close the **Network Connections** window.

## Installing Hitachi Device Manager - Storage Navigator

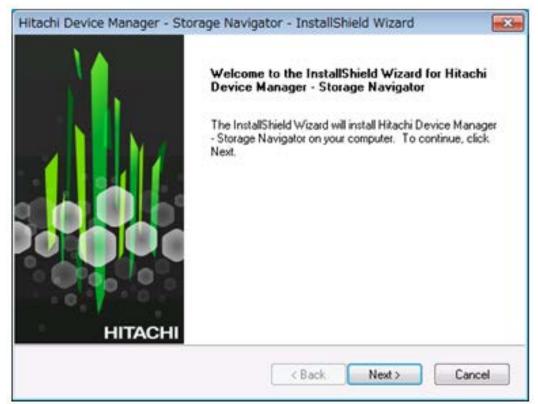
The procedure for installing the Device Manager - Storage Navigator software takes approximately 10 minutes.

#### Procedure

- 1. Connect a PC to the LAN2 port on the SVP.
- 2. Insert the attached SVP firmware media into the PC's CD drive or DVD drive.
- **3.** On the root folder of the SVP firmware media, right-click **Setup.exe**, and then click **Execute as Administrator**.
- 4. In the Choose Setup Language window, click a language, and then click Next.

Hitachi Device Manager - St	torage Navigator - InstallShield Wi	zard 🕞 🖻 🔜
Choose Setup Language Select the language for the in	nstallation from the choices below.	24
(English (United States) Japanese		
InstallShield	< gack Next	> Cancel

The **Preparing Setup** window appears while the software is prepared for installation.



5. At the Install Shield window, click Next.

6. At the License Agreement window, accept the terms of the license agreement, and then click Next.

Hitachi Device Manager - Storage Navigator - InstallShield Wizard	X
License Agreement Please read the following license agreement carefully.	4
Apache License Version 2.0, January 2004 http://www.apache.org/licenses/	-
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.	
"Licensor" shall mean the copyright owner or entity authorized by	-
I goccept the terms of the license agreement     Did not accept the terms of the license agreement InstallShield	
Next > Car	icel

 At the next window, specify the folder where Device Manager - Storage Navigator will be installed. Either accept the default folder shown in the window or click Browse to select a different folder.

Hitachi Device Manager - Storage Navigator	
Choose Destination Location Select folder where setup will install files.	1
Select rober where setup will install tiles.	
Setup will install Hitachi Device Manager - Storage Navig	ator in the following folder.
To install to this folder, click Next. To install to a different f another folder.	folder, click Browse and select
Destination Folder	
C:\Mapp	Browse
InstallShield	
	OK Cancel

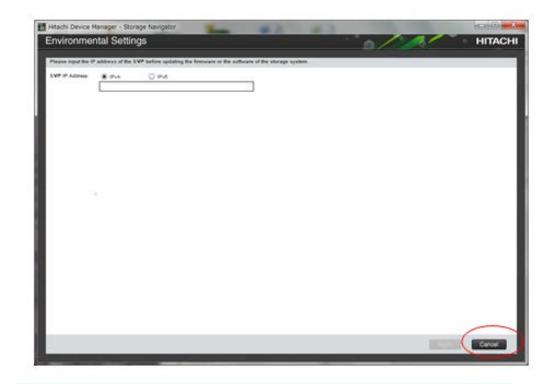
**8.** If a confirmation window appears, click **Yes**. If the Windows Security Alert window appears, click **Allow access**.

A status bar shows the progress of the installation.

- **9.** When the following completion message appears, perform one of the following steps:
  - To continue, click **The setting has been completed**. I will continue installation and updating of the software.
  - To set port numbers, firewall settings, and anti-virus software, click The setting is not completed. I will install and update the software after I complete the setting.

	InstallShield Wizard Complete Install is completed.Set the below items. [1]Port# [2]Firewall
HITAC	<ul> <li>(3)Anti virus soft you must start up service processes of Storage Navigator, after you must start up service processes of Storage Navigator, after updating of the software.</li> <li>The setting has been completed.1 will install and update the software later.</li> <li>The setting is not completed.1 will install and update the software after 1 complete the setting.</li> </ul>

- 10. Click Finish.
- **11.** At the **Environmental Settings** window, click **IPv4** or **IPv6**, and then enter the IP address of the SVP and click **Apply**.



**Note:** If you do not want to configure the SVP IP address at this time, click **Cancel**. When you are ready to specify the IP address, restart the SVP, and then set the SVP IP address using the procedure under <u>Setting</u> the IP address (on page 255).

Ē

## **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

- 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.

Chapter 20: Troubleshooting

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

Chapter 20: Troubleshooting

# 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	HDW2-F850-SVP.P
	VSP F350 and VSP F370	
	VSP G700	
	VSP F700	
	VSP G900	HDW-F850-SVP.P
	VSP F900	
	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

Appendix A: SVP replacement list

## Hitachi Vantara Corporation



Corporate Headquarters 2845 Lafayette Street Regional Contact Information

Americas: +1 866 374 5822 or info@hitachivantara.com

Santa Clara, CA 95050-2639 USA

Americas: +1 866 374 5822 or into@nitacnivantara.com

Europe, Middle East, and Africa: +44 (0) 1753 618000 or info@emea@hitachivantara.com

www.HitachiVantara.com | community.HitachiVantara.com Asia Pacific: + 852 3189 7900 or info.marketing.apac@hitachivantara.com