

HITACHI

VSP One Block Security Hardening Best Practices

MK-26VSP1B041-00 April 2026

Table of contents

1	Executive summary	5
2	Introduction	5
2.1	<i>Embedded System Manager</i>	5
2.2	<i>Storage array system security</i>	5
2.3	<i>Best practice security deployment checklist</i>	6
3	System hardening topics	6
3.1	<i>Physical security</i>	6
3.2	<i>Data protection</i>	6
3.2.1	Data-at-rest encryption	7
3.2.2	External key management server	7
3.2.3	Encryption environmental settings	7
3.2.4	Resource partitioning	8
3.2.5	LUN security	9
3.2.6	Namespace security	9
3.2.7	iSCSI CHAP	9
3.2.8	Media sanitization	9
3.3	<i>Network security</i>	10
3.3.1	Architecture overview	10
3.3.2	Firewall configuration	11
3.3.3	Transport Layer Security	12
3.4	<i>Authentication and access controls</i>	13
3.4.1	Role-based access control	13
3.4.2	External user authentication server	13
3.4.3	Disable local user accounts or change local account passwords	14
3.5	<i>Hardware root of trust and secure firmware update</i>	15
4	Customer service and system updates	15
4.1	<i>Customer service</i>	15
5	System auditing and monitoring	15
5.1	<i>Configure the VSP to transfer logs to an external syslog server</i>	15
5.2	<i>Monitoring system events via SNMP</i>	16
6	Conclusion	16

Notices and Disclaimer

© 2026 Hitachi Vantara LLC. All rights reserved.

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

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 to access relevant data; and
- 2) Verifying that 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.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

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, Flash Copy, IBM, Lotus, MVS, OS/390, PowerPC, RS6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, BCPII™ 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.

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

IMPORTANT: This document can only be used as Hitachi Vantara internal documentation for informational purposes only. This documentation is not meant to be disclosed to customers or discussed without a proper non-disclosure agreement (NDA).

About this document

Introduction

This document describes the Hitachi Virtual Storage Platform One Block storage systems (VSP One B20 series, VSP One B80 series) security configuration best practices.

Intended audience

This document is intended for employees, partners, and customers who use VSP One Block storage systems.

Document revision

Revision number	Date	Details
v1.0	April 2026	Initial release

Comments

Send any comments on this document to Docs-Feedback@hitachivantara.com. Include the document title, including the revision level, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you.

1 Executive summary

This paper focuses on the numerous security features built into the Hitachi Virtual Storage Platform One Block storage systems to protect and secure data, access, and communications. These features are designed to help administrators and network engineers deploy VSP One Block storage systems to minimize vulnerabilities and threat exposure.

The VSP One Block storage systems include multiple layers of security that protect physical, network, and data access. Other security features include use of custom certificates, data-in-flight encryption, and data-at-rest encryption.

Configurable security features covered in this paper include:

- **Role-Based Access Controls:** Configure user permissions by giving groups defined roles to perform their responsibilities with the least required privileges.
- **Resource Partitioning:** Ensure that resources are partitioned and data management permissions are assigned to users in only their own resource group.
- **Data-at-Rest Encryption:** Enable FIPS-certified Data-at-Rest Encryption.
- **Support for external key management:** Enable external KMIP-compliant key management server (KMS) for enterprise management of encryption keys.
- **Data-in-Flight Encryption:** Configure TLS encryption including installing certificates for the Web Server, SMI-S, RMI and REST API.
- **User authentication:** In addition to local user accounts, enterprise identity services: LDAP is supported.
- **Network firewall:** Configure any firewalls protecting the VSP storage system to ensure only required ports and protocols are allowed to connect to the storage system.
- **Audit logging:** Full support for both UDP- and TLS-encrypted TCP remote syslog servers.
- **Hardware Root of Trust:** Utilizes a digital signature to verify the integrity and authenticity of all firmware images.
- **Secure firmware update:** The VSP One Block implements secure boot that detects firmware corruption and prevents the booting of corrupted firmware.

2 Introduction

2.1 Embedded System Manager

The VSP One Block storage systems come equipped with an Embedded System Manager (ESM). This ESM hosts the web-based element manager GUI and accepts CLI and API commands.

Security assessments and audits are performed periodically on the VSP storage systems, including network vulnerability scans using industry-standard security scanning tools as well as penetration tests.

Other aspects of storage system hardening include the following elements:

- Disabling all services not required for storage system operation to minimize the attack surface of the EMS
- Utilizing industry best practices for core configuration of the ESM, including internal firewalls, limiting permissions, and configuring local settings to provide protection in depth against malicious users and software

2.2 Storage array system security

The VSP storage systems back-end components are highly secured devices with extremely limited outside access. Remote access to the system is limited to the pre-defined API calls over controlled interfaces. There is no unconfined console level access remotely to the storage systems.

2.3 Best practice security deployment checklist

The following list is a summary of best practices a consumer should take to ensure the highest level of security.

Physical Security

- Limit physical VSP hardware access to a minimum set of trusted and qualified individuals by locking the rack and the room in which it resides.
- Ensure the back-end network utilizes non-routable addresses and prohibits any outside connections.

Data Protection

- Enable data-at-rest encryption to safeguard sensitive data from accidental disclosure. (This is the default configuration on the VSP One Block and newer systems.)
- External encryption key management
- Resource partitioning
- LUN security
- Namespace security
- iSCSI CHAP
- Media sanitization

Network Security

- Review port requirements and firewall unused ports on management network.
- Configure cryptographic algorithms supported for data-in-flight TLS encryption.
- Disable HTTP access (this is the default configuration on the VSP One Block and newer systems).
- Install certificates for HTTPS, RMI, SMI-S, and REST API.
- Ensure Network Time Protocol (NTP) has authoritative sources.
- Enable HTTP Strict Transport Security (HSTS).

Authentication and access controls

- Take a least-privileges approach to assigning role-based access controls.
- Use external enterprise authentication.

System administration and configuration

- Keep VSP firmware updated to ensure the latest bug fixes and Common Vulnerabilities and Exposures (CVE) protections.
- Configure syslog to external logging.
- Configure SNMP.

3 System hardening topics

3.1 Physical security

Physical security is primarily a customer issue; the customer should ensure that VSP is installed in their data center with the following in mind:

- Limit administrative access to a minimum set of trusted and qualified individuals.
- Confirm non-routable addresses are used for the back-end network and prohibit any outside connections.
- Consider data-at-rest encryption to safeguard sensitive data from accidental disclosure.

3.2 Data protection

Data must be protected both at rest and in flight to ensure the confidentiality and integrity of the data stored on the VSP One Block storage systems. To achieve this goal for the data stored on the arrays, data-at rest encryption should be enabled on all volumes utilizing an external key

management server, permissions on storage resources should be partitioned, the logical volumes should be secured, and iSCSI CHAP authentication should be configured.

3.2.1 Data-at-rest encryption

VSP One Block storage systems provide a performance-friendly FIPS-certified AES-256-XTS encryption capability on the back-end I/O module. This capability protects data at rest on internal storage media (flash drives). If data is encrypted, information leakage is prevented when the storage system or the drives in the storage system are replaced. Likewise, the VSP encryption capability provides an extra measure of protection and confidentiality for lost, stolen, or misplaced media that may contain sensitive information. It provides a unique encryption key for each piece of media internal to the array. VSP storage systems can also use data-at-rest encryption to provide cryptographic erasure of data. This technique is much more efficient than traditional overwrite methods and works for flash drives and drives that have failed.

The Encryption License Key feature provides the following benefits:

- Encryption can be applied to some or all supported internal volumes.
- Each encrypted internal drive is protected with a unique data encryption key.
- Encryption has negligible effects on I/O throughput and latency.
- Encryption requires little to no disruption of existing applications and infrastructure.

For more details about the data-at-rest encryption, see the Encryption License Key User Guide for VSP One Block.

3.2.2 External key management server

Utilize an external KMS to store and manage the encryption keys for the VSP One Block storage system. Using an external KMS enables you to easily back up and restore encryption keys, to remove keys from the array on power off, and to quickly and easily re-key the key encryption key (KEK) if desired.

Requirements:

External KMIP-compliant (v1.0 - v1.4) key management server such as:

- Thales CipherTrust Manager / SafeNet KeySecure
- Vormetric Data Security Manager (DSM)
- Micro Focus Enterprise Secure Key Manager (ESKM)
- IBM® Security Key Life Manager

For the latest information about supported key management servers, see the Encryption Key Management Server Support Matrix on the interoperability site:

<https://compatibility.hitachivantara.com/products/ekms>

3.2.3 Encryption environmental settings

The encryption environmental settings enable users to tailor the encryption settings for their environment, including network settings, connection settings for the key management servers, disabling local key creation, and encryption key backups. To protect the key encryption key (KEK) at the key management server, you can configure a secondary key management server when you configure the encryption environmental settings.

If encryption keys are stored in the key management server, you can configure the encryption keys in the storage system to be deleted when the storage system is powered off.

Table 1: KMS Configuration

#	KMS	Generate Keys on the KMS	Protect KEK at the KMS	Delete Internal Encryption Keys at Power Off	Disable Local Key Generation	Notes
1	No	N/A	N/A	N/A	N/A	Internal key management, no KMS
2	Yes	No	No	No	No	KMS used as secondary key backup only

#	KMS	Generate Keys on the KMS	Protect KEK at the KMS	Delete Internal Encryption Keys at Power Off	Disable Local Key Generation	Notes
3	Yes	Yes	No	No	No	KMS used for key creation and for secondary key backup
4	Yes	Yes	Yes	No	No	KMS used to generate and store secondary backup of keys KEK not saved on array and must be downloaded on power on of the array to decrypt the local primary backup.
4a	Yes	Yes	Yes	No	Yes	Same as 4, but local key generation permanently disabled.
5	Yes	Yes	Yes	Yes	No	KMS used to generate and store all keys. Keys are never saved locally on the storage system and must be downloaded from the KMS when the array is powered on.
5a	Yes	Yes	Yes	Yes	Yes	Same as 5, but local key generation is permanently disabled.

3.2.4 Resource partitioning

- You can divide a provisioned storage system into resource groups that allow you to manage the storage system as multiple virtual private storage systems. Configuring resource groups involves creating resource groups, moving storage system resources into the resource groups, and assigning resource groups to user groups.
- A storage system can connect to multiple hosts and be shared by multiple divisions in a company or by multiple companies. Many storage administrators from different organizations can access the storage system. Managing the entire storage system can become complex and difficult. Potential problems are that private data might be accessed by other users, or a volume in one organization might be accidentally destroyed by a storage administrator in another organization.
- To avoid such problems, use Resource Partition Manager software to set up resource groups that allow you to manage one storage system as multiple virtual private storage systems. The storage administrator in each resource group can access only their assigned resources. Resource groups prevent the risk of data leakage or data destruction by another storage administrator in another resource group.
- Each resource group is assigned a number (RSG number) for identification. Also, each resource group is assigned to a user group and each storage resource administrator can perform management operations within the range of resource groups assigned to the user group the administrator belongs to. As all resource groups are assigned to maintenance personnel, they can perform maintenance for all storage resources.
- When a user logs into the embedded user interfaces (VSP One Block Administrator and Maintenance Utility), that user's access privileges determine the resources they can view and the operations they can perform. User access privileges are determined by the user groups to which a user belongs and the resources assigned to those user groups. To perform an operation on the storage system, they must have access to the resources (for example, volumes, pools, ports) that are required for the operation.
- Information on how to create resource groups and assign permissions to manage resource groups can be found in the [System Administrator Guide](#). One key security requirement for resource groups is a user with the security administrator role and the storage administrator role with the "All Resource Groups Assigned" set to yes. That user can edit storage access for all resource groups.

Do not give the storage administrator role with the "All Resource Groups Assigned" flag set to anyone with the security administrator role.

3.2.5 LUN security

To protect mission-critical data in your storage system from unauthorized access, secure the logical volumes in the storage system. For VSP One Block storage systems, you can protect LUs from unauthorized access by enabling LUN security on ports.

3.2.6 Namespace security

NVMe over Fabrics (NVMe-oF) is an extended protocol that enables communication over a Fibre Channel fabric or an Ethernet fabric with NVMe. NVMe-oF enables the use of namespace security functions instead of LUN security, which uses the conventional Fibre Channel (FC-SCSI) connection. To use namespace security functions, you must enable the namespace security setting on the NVM subsystem. You do not need to configure the LUN security setting for a Fibre Channel port.

When namespace security is enabled, a logical volume that the host can access is determined by the host NQN settings for the NVM subsystem and the namespace. The host can only access a logical volume assigned to the NVM subsystem and the namespace for which the host NQN is set.

3.2.7 iSCSI CHAP

When a host sends a login request to the VSP One Block storage system, the storage system judges whether to permit or reject the login request according to iSCSI CHAP authentication. CHAP users should be given the least privilege required to function.

3.2.8 Media sanitization

Shredding

The Volume Shredder software for VSP One Block storage systems enables you to securely erase data on volumes by overwriting existing data to prevent restoration of the erased data. For example, when the user of a volume changes, you may want to purge the data stored by the previous user before giving access to the new user. This method of erasing data by overwriting it with dummy data is referred to as shredding.

Because of the way data is written on the drives, overwriting data once or twice might not be enough to ensure that the data cannot be restored. The best practice is to overwrite data at least three times with dummy data. Volume Shredder allows you to specify the number of times the data is overwritten, enabling you to ensure compliance with applicable requirements (for example, DoD5220.22-M). The procedures for volume shredding can be found on the Hitachi Vantara documentation portal.

Note: Complete data erasure can be guaranteed only for hard disk drives (HDDs). For flash drives (for example, SSDs, SCMs), complete data erasure (overwriting all cells including overprovisioned cells) cannot be guaranteed. You can use Cryptographic Erasure (see below) or Hitachi Data Eradication Services (contact customer support for more information).

Cryptographic erasure

ISO/IEC 27040:2015 (Information technology – Security techniques – Storage security) and NIST Special Publication 800-88 Revision 1 (Media Sanitization) define a data/media sanitization technique known as cryptographic erase, which can be used to purge data by irrevocably destroying appropriate keys (for example, DEKs, MEKs, etc.). This technique is extremely fast when compared to traditional overwrite techniques and it is effective with flash technologies that employ overprovisioning features that cannot be reliably cleared using overwrites as well as with drives that are failing or have failed and cannot accept I/Os.

VSP One Block storage systems automatically employ cryptographic erasure as part of the following operations to protect data:

- Drive Removal – When an encrypted drive that is connected to an encryption module (ENCM) with the encryption environment settings initialized (i.e., keys have been generated) is removed, the DEK associated with that drive is zeroed, which renders all data on the drive unrecoverable. If that same drive is reinstalled in the original VSP One Block storage system, a new DEK is assigned to it; it is not possible to force a recovery of the old DEK from a previous key backup and use it with the reinstalled drive.

- Disable Parity Group Encryption – When encryption on a parity group is disabled, the DEKs associated with each drive in the parity group are zeroed and then a new DEK is assigned for each drive. It is important to note that disabling encryption can only occur after all the LUs have been removed and I/O is blocked – this cannot be used as an attack vector to destroy data.
- Initialize Encryption Environment Settings – When the encryption environment settings are initialized on a VSP One Block storage system with ENCMs, all the keys are zeroed. A subsequent configuration of the encryption environment settings will cause new keys to be generated with DEKs being assigned to each drive connected to the initialized ENCM.

3.3 Network security

3.3.1 Architecture overview

Administrators of the VSP One Block storage systems access the management interfaces using Ethernet technology. The following figure shows how a VSP storage system fits into a customer network.

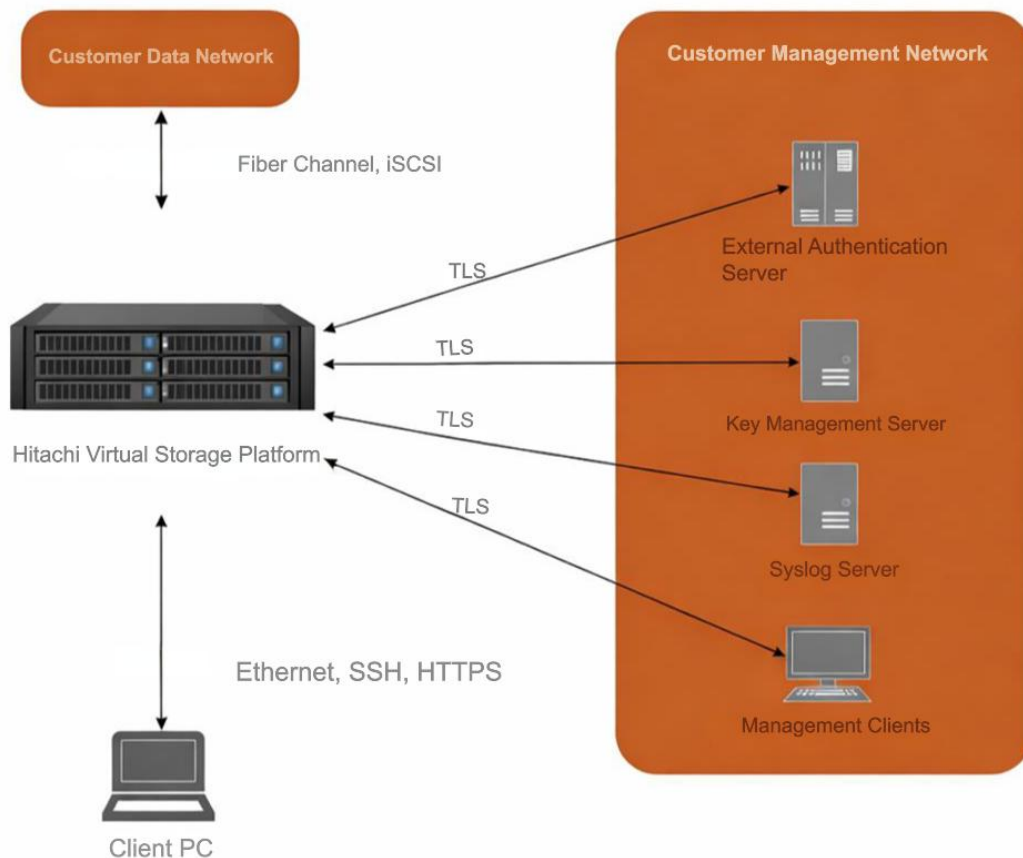


Figure 1: Enterprise VSP network diagram

Private back-end network: There is a private network that is used for command and control of the VSP's various components. This network is physically separate from the customer's network, only connecting the Maintenance PC to the storage controllers. Follow these guidelines to ensure the security of this network:

- Configure non-routable addresses (10.0.0.0/8, 172.16.0.0/12 (default), 192.168.0.0/16) for the back-end network.
- Never connect the VSP back-end switches to any other computer systems or networking gear.
- Limit physical access to the VSP nodes, switches, and storage arrays to authorized personnel.

Management network: The VSP One Block storage systems provide connections to/from the following management services on the customer's management network:

Services provided by VSP:

- Virtual Storage Platform One Block Administrator
- Maintenance utility
- REST API
- Web Console (limited to Hitachi maintenance personnel/CEs only)

Services used by VSP:

- Syslog
- DNS
- External encryption key management (KMIP)
- Authentication and authorization services (Kerberos/LDAP)
- NTP

Storage connections: Connections to the storage array are independent of the customer network. This is by design to ensure the confidentiality and integrity of the data stored on the storage array.

3.3.2 Firewall configuration

VSP deployment in the environment relies on two tiers of firewall to provide in-depth protection. This is accomplished through the customer-managed data center firewall.

Management network firewall

VSP One Block storage systems are often deployed behind a corporate firewall; limiting access to the VSP management network remains an important part of the security strategy. Network engineers responsible for administrating the front-end switch may elect to restrict port utilization to a minimum set required by VSP. The following table presents a list of ports the VSP might need during operation. The actual needs vary by specific deployment needs such as NTP, external authentication servers, KMS servers, and so on.

Table 2: VSP port requirements

Port	Type	Direction	Protocol	Notes
80	TCP	Inbound	HTTP	Disabled by default on VSP One Block and newer
443	TCP	Inbound	HTTPS	
11099	TCP	Inbound	RMI Registry Server	
51099	TCP	Inbound	RMI	
51100	TCP	Inbound	RMI	
427	TCP	Inbound	SMI-S	
5989	TCP	Inbound	SMI-S (CIMOM)	
161	TCP	Inbound	SNMP	
162	TCP	Outbound	SNMP Trap	
31xxx	TCP	Inbound	Command Control Interface	
34xxx	TCP	Outbound	Command Control Interface	
5443	TCP	Inbound	HTTPS (raidinf)	
23454	TCP	Outbound	Configuration Manager REST API	
5696	TCP	Outbound	KMIP	Connection to external KMS Server

Port	Type	Direction	Protocol	Notes
443	TCP	Outbound	HTTPS	(Optional) Connection to HRO
2056	TCP	Inbound	HRO Communication	(Optional) Connection to HRO Site Manager
2057	TCP	Inbound	HRO Communication	(Optional) Connection to HRO Site Manager

3.3.3 Transport Layer Security

Use strong encryption when transmitting data across the network. The VSP uses the Transport Layer Security protocol (TLS 1.2 and 1.3) to ensure privacy and data integrity between the VSP and other systems with which it communicates. TLS is the successor to the Secure Sockets Layer (SSL) cryptographic protocol. TLS provides data-in-flight encryption utilizing HTTPS for VSP services including RMI, the Web Interface, SMI-S, and the REST API.

Server encryption certificates (HTTPS, PF Rest, and RMI)

For HTTPS communication, the VSP maintains a server certificate utilized by the web services. This certificate initially is a Secure Hash Algorithm 2 (SHA-2) self-signed certificate and generated at installation time. Organizations can also generate a new certificate to replace the one generated at installation to either update the details or replace an expired certificate.

The following table lists the ports to which the Server Encryption Certificate applies.

Table 3: Ports to which the Server Encryption Certificate applies

Protocol	Port Number
HTTPS	443
RMI registry	11099
RMI (SSL)	5443
RMI	51100

TLS protocols and encryption algorithms

The TLS cipher algorithms are modifiable to ensure only the latest and most secure encryption is available at any time. **Disable all CBC-based cipher suites and enable only the most secure cipher options required for your environment.**

Disable HTTP access

Once the storage system is using TLS (HTTPS), the HTTP setting tool allows you to block access to port 80. When you block access to port 80, all web traffic is routed through port 443. HTTP is disabled by default.

SMI-S encryption certificates

To enable encryption on the SMI-S interface, an encryption certificate containing an encryption key is uploaded to the storage system. The signed server certificate (public key) is installed.

NTP

To ensure accurate timestamps in logs as well as certificate validity, an accurate time source is pivotal. If an NTP server exists on the management network, the VSP should be configured to retrieve time from it. This procedure can be performed only by authorized maintenance personnel. Contact customer support for more information.

HTTP Strict Transport Security (HSTS)

HSTS is a security function in which the web server informs the web browser to use HTTPS. The Management Client can be configured to enable HSTS when HTTP communication isn't completely blocked. This procedure can be performed only by authorized maintenance personnel. Contact customer support for more information.

3.4 Authentication and access controls

The VSP storage system has robust user authentication using both local and standard authentication frameworks such as Active Directory.

The following subsections outline these key security features.

3.4.1 Role-based access control

The VSP storage system is delivered with several default roles that can be assigned to different users and user groups. These roles can be customized by the customer to either limit or expand their permissions to suit their security requirements.

- **Security administrator**

The security administrator can register, modify, and delete administrator accounts using the element-manager user interface (UI) software (Maintenance Utility, Storage Navigator). Also, the administrator can assign the management authority of the group of storage resources, called a “resource group”, to a specific user. In addition to the above, the administrator can make an identification setting for the host, make identification and authentication settings for the Fibre Channel switch, and perform an encryption operation on stored data.

- **Storage resource administrator**

The storage resource administrator can manage resources assigned to the security administrator (such as port, cache memory, and drives) by using the element manager software.

- **Audit log administrator**

The audit log administrator can manage audit logs stored in the storage systems. The administrator can view and download the audit logs and make settings related to syslog using the element-manager software.

- **User Maintenance**

Maintenance personnel belong to a group specializing in maintenance of the storage system and with whom customers sign maintenance contracts. They are responsible for the initial startup process in installing the storage system, changing settings required in maintenance activities such as parts replacement or addition, and disaster recovery. Only maintenance personnel can directly access the components inside the storage system and operate devices connected to the internal LAN. All resources of the storage system are assigned to the maintenance personnel, and they can perform operations allowed by the maintenance role.

- **Storage user**

The storage user is the user of the storage system (represents a host) who accesses the data stored in the storage system through the hosts connected to the storage system.

For details about supported roles and permissions, see the [System Administrator Guide](#) for your storage system.

3.4.2 External user authentication server

The VSP storage systems validate users with any of the following authentication methods:

- Local authentication
- LDAP

Utilize LDAP for all user authentication.

The following figure shows the login workflow with an external authentication server.

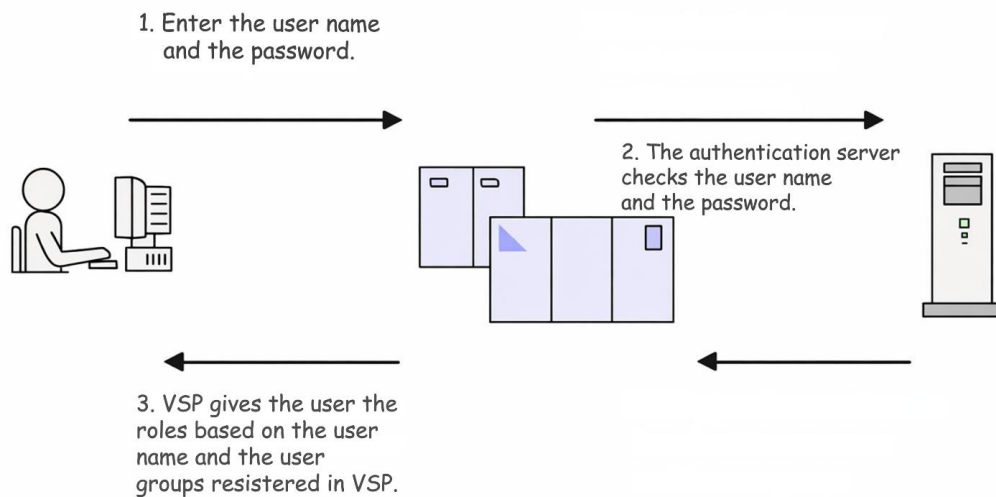


Figure 2: Login workflow with an external authentication server

If an authorization server works together with an authentication server, the user groups that are registered in the authorization server can be assigned to storage system users.

The following figure shows the login workflow when an authentication server and an authorization server are used in combination.

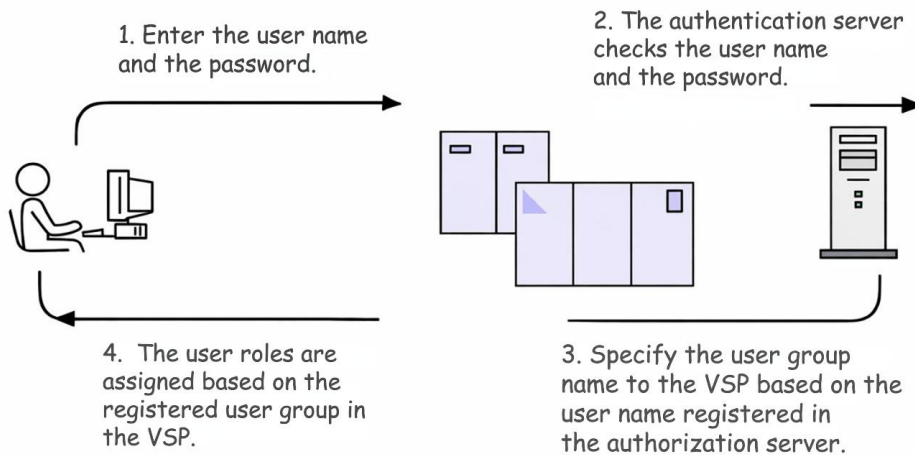


Figure 3: Login workflow when an authentication server and an authorization server are used in combination

If you register the information of the authentication server as a service record (SRV) on the DNS server, you can use the authentication server without knowing the host names and port numbers. If you register multiple authentication servers to the SRV, you can determine the authentication server to be used based on the priority that has been set in advance.

Note: Two authentication servers (one primary and one secondary) can be connected to a storage system. In this case, the server configurations must be the same, except for the IP address and port number.

To configure, External Authentication users can access this by clicking **Administration > External Authentication > Set Up Server > LDAP**.

3.4.3 Disable local user accounts or change local account passwords

You should disable the built-in user accounts once the storage system is connected to an external authentication server. This ensures that all user access is managed via the customer's enterprise network.

3.5 Hardware root of trust and secure firmware update

The VSP One Block storage systems implement secure boot that detects firmware corruption and prevents the booting of corrupted firmware. When the ESM boot loader detects FW corruption, the ESM restores the firmware image from the golden image after booting with redundant normal FW. The golden image also has a digital signature.

The VSP One Block uses a digital signature mechanism to verify the integrity and authenticity of all firmware images when ESM downloads firmware.

VSP One Block storage systems do not support installation of third-party antivirus or endpoint protection software. Malware protection is achieved through system hardening, service minimization, secure boot, and digitally signed firmware updates.

4 Customer service and system updates

4.1 Customer service

All customers should register with the Hitachi Vantara Support website. By doing so, customers can subscribe to receive Technical Bulletins to stay informed of critical product and security alerts. Failure to register with Hitachi Vantara Support and subscribe to Technical Bulletins may result in not receiving important Technical Bulletins or other alerts. Please visit Hitachi Vantara's Support Site to register and subscribe.

An important design aspect of Hitachi's storage architecture is the separation of the data access from management access. This feature provides tools and interfaces that are used to configure, monitor, and manage one or more storage systems, and none of these tools or interfaces can directly access data stored on the storage system.

Maintenance agreement

Ensuring the VSP storage system gets regular security patches and microcode updates is a vital part of the ongoing security of the storage system. Maintaining an agreement provides access to the following offerings:

- Hitachi maintenance manuals
- Hitachi-certified parts and parts depots
- Hitachi Customer Engineer (CE) assistance in the field
- Hitachi Global Support Center (HGSC)
- Hitachi troubleshooting resources and contacts
- Hitachi engineering resources and contacts
- Hitachi alerts associated with Global Customer Support Services
- Hitachi microcode and firmware updates

In addition, complex repair tasks, including but not limited to pinned data, LDEV blocking, and so on, cannot be accomplished without unique passwords from Hitachi Engineering along with specific Hitachi software tools to complete the task. These resources are included only with Global Customer Support Services.

5 System auditing and monitoring

The VSP storage system supports external monitoring via syslog, SNMP, and email. For enterprise-level monitoring, use both syslog and SNMPv3 to ensure system critical events are responded to as quickly as possible.

5.1 Configure the VSP to transfer logs to an external syslog server

The VSP One Block storage systems support secure audit logging using the syslog protocol to remotely offload real time logs to ensure all operations and events are traceable both locally and remotely. This security audit logging capability takes advantage of Transmission Control Protocol (TCP) and Transport Layer Security (TLS) for reliable delivery and security of audit logging

information. It keeps the information secure while it is transferred from the storage system to the organization's event management infrastructure. VSP storage systems also maintain legacy support for User Datagram Protocol-based (UDP-based) audit logging, so it is backward compatible with previous generations of syslog and legacy event management tools.

You can select either of the following protocols to transfer the audit log to the syslog server. The output file format is different depending on the selected protocol:

- TLS/RFC5424 (Recommended)
- UDP/RFC3164

5.2 Monitoring system events via SNMP

Simple Network Management Protocol (SNMP) is an industry-standard protocol for managing and monitoring network devices, including data drives, routers, and hubs. SNMP uses Simple Gateway Management Protocol (SGMP) to manage TCP/IP gateways.

The SNMP Agent collects error information, usage conditions, and other information about the array and reports storage system failures to the SNMP manager using the SNMP trap function. The SNMP Agent runs on the storage system and communicates with the SNMP manager through the LAN between the storage system and the SNMP manager.

Caution: Use SNMP version 3 due to underlying security issues with SNMP versions 1 and 2 protocols.

6 Conclusion

Hitachi Virtual Storage Platform storage systems are designed with robust security features to ensure a safe and secure storage platform. Data security requirements now permeate every aspect of the storage infrastructure. Whether data is stored as a file, a block, or an object, security must be enforced throughout the entire storage ecosystem. Hitachi Virtual Storage Platform family of hybrid models and all-flash arrays, along with our file and content offerings, provides the necessary components to address the most stringent data security needs.

Many organizations must address specific regulatory and compliance directives such as the Payment Card Industry Data Security Standard (PCI-DSS), General Data Protection Regulation (GDPR), and the Health Insurance Portability and Accountability Act (HIPAA). In addition to specific requirements such as these, general concerns regarding data security and the handling of sensitive information must also be addressed.

The advanced security features of the VSP storage systems enable customers to address and meet all these challenges. By following the recommendations in this document, organizations can build and maintain an enterprise-class repository infrastructure to support the needs of multiple applications.