

# Antivirus Administration Guide

---

Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS  
Modules

VSP N series

Hitachi NAS Platform

Release 14.2

© 2011, 2019 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 LLC (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 LLC 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 LLC.

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 and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Edge, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft corporate logo, the Microsoft Edge 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 website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found at <https://www.hitachivantara.com/en-us/company/legal.html>.

---

# Contents

Preface .....	4
Related Documentation.....	4
Accessing product documentation.....	7
Getting help.....	7
Comments.....	7
<b>About virus scanning.....</b>	<b>9</b>
Virus scanning overview.....	9
Using the Internet Content Adaption Protocol (ICAP).....	11
Configuring virus scan engines.....	12
Compatibility with SMB3 Multichannel.....	12
Enabling virus scanning on the storage server.....	12
Forcing files to be rescanned.....	16
Enabling an exclusion list.....	17
Enabling maximum file size for virus scanning.....	17

# Preface

This guide describes the supported antivirus engines, provides information about how to enable them, and how to configure the system to use them. Note that some features apply only to individual platforms and may not be applicable to your configuration.

Virtual Storage Platform G400, G600, G800 and Virtual Storage Platform F400, F600, F800 storage systems can be configured with NAS modules to deliver native NAS functionality in a unified storage platform. The term 'NAS module' in this document also applies to VSP F series, VSP G series, and VSP N series. The unified VSP Gx00 models, VSP Fx00 models, and VSP N series models automatically form a two-node cluster in a single chassis upon installation, with no external cabling required.

## Related Documentation

**Release Notes** provide the most up-to-date information about the system, including new feature summaries, upgrade instructions, and fixed and known defects.

### Command Line References

The Command Line Reference provides information on the commands used to manage your system, and includes relevant information on the operation of your hardware and software. Depending on the model of your server or cluster node, refer to the Command Line Reference that is appropriate for your system.

- *NAS Module Server Command Line Reference*
- *Command Line Reference for models 4060, 4080, and 4100*
- *Command Line Reference for models 3080, 3090 and 4040*
- *Command Line Reference for models 5200 and 5300*

## Administration Guides

- *System Access Guide* (MK-92HNAS014)—Explains how to log in to the system, provides information about accessing the NAS server/cluster CLI and the SMU CLI, and provides information about the documentation, help, and search capabilities available in the system.
- *Server and Cluster Administration Guide* (MK-92HNAS010)—Provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading software, monitoring servers and clusters, and backing up and restoring configurations.
- *Storage System User Administration Guide* (MK-92HNAS013)—Explains user management, including the different types of system administrator, their roles, and how to create and manage these users.
- *Network Administration Guide* (MK-92HNAS008)—Provides information about the server's network usage, and explains how to configure network interfaces, IP addressing, name and directory services.
- *File Services Administration Guide* (MK-92HNAS006)—Explains about file system formats, and provides information about creating and managing file systems, and enabling and configuring file services (file service protocols).
- *Data Migrator Administration Guide* (MK-92HNAS005) —Provides information about the Data Migrator feature, including how to set up migration policies and schedules.
- *Storage Subsystem Administration Guide* (MK-92HNAS012)—Provides information about managing the supported storage subsystems (RAID arrays) attached to the server/cluster. Includes information about tiered storage, storage pools, system drives (SDs), SD groups, and other storage device related configuration and management features and functions.
- *Snapshot Administration Guide* (MK-92HNAS011)—Provides information about configuring the server to take and manage snapshots.
- *Replication and Disaster Recovery Administration Guide* (MK-92HNAS009)—Provides information about replicating data using file-based replication and object-based replication, provides information on setting up replication policies and schedules, and using replication features for disaster recovery purposes.
- *Antivirus Administration Guide* (MK-92HNAS004)—Describes the supported antivirus engines, provides information about how to enable them, and how to configure the system to use them.
- *Backup Administration Guide* (MK-92HNAS007)—Provides information about configuring the server to work with NDMP, and making and managing NDMP backups.



**Note:** For a complete list of Hitachi NAS open source software copyrights and licenses, see the *System Access Guide*.

## Hardware References

- *Hitachi NAS Platform 3080 and 3090 G2 Hardware Reference* (MK-92HNAS017) — Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- *Hitachi NAS Platform and Hitachi Unified Storage Series 4000 Hardware Reference* (MK-92HNAS030)—Provides an overview of the Hitachi NAS Platform Series 4000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components
- *Hitachi NAS 5000 Series Hardware Reference* MK-92HNAS089—Provides an overview of the Hitachi NAS Platform Series 5000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.
- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.

## Best Practices

- *Hitachi NAS Platform Best Practices Guide for NFS with VMware vSphere* (MK-92HNAS028)—This document covers best practices specific to using VMware vSphere with the Hitachi NAS platform.
- *Hitachi NAS Platform Deduplication Best Practice* (MK-92HNAS031)—This document provides best practices and guidelines for using deduplication.
- *Hitachi NAS Platform Best Practices for Tiered File Systems* (MK-92HNAS038)—This document describes the Hitachi NAS Platform feature that automatically and intelligently separates data and metadata onto different Tiers of storage called Tiered File Systems (TFS).
- *Hitachi NAS Platform Data Migrator to Cloud Best Practices Guide* (MK-92HNAS045)—Data Migrator to Cloud allows files hosted on the HNAS server to be transparently migrated to cloud storage, providing the benefits associated with both local and cloud storage.
- *Best Practices for Hitachi NAS Universal Migrator* (MK-92HNAS047)—The Hitachi NAS Universal Migrator (UM) feature provides customers with a convenient and minimally disruptive method to migrate from their existing NAS system to the Hitachi NAS Platform. The practices and recommendations outlined in this document describe how to best use this feature.
- *Hitachi Data Systems SU 12.x Network File System (NFS) Version 4 Feature Description* (MK-92HNAS056)—This document describes the features of Network File System (NFS) Version 4.
- *Hitachi NAS HDP Best Practices* (MK-92HNAS057)—This document lists frequently asked questions regarding the use of Hitachi Dynamic Provisioning.
- *Hitachi Multi-tenancy Implementation and Best Practice Guide* (MK-92HNAS059)—This document details the best practices for configuring and using Multi-Tenancy and related features, and EVS security.
- *Hitachi NAS Platform HDP Best Practices* (MK-92HNAS063)—This document details the best practices for configuring and using storage pools, related features, and Hitachi Dynamic Provisioning (HDP).

- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.
- *NAS Platform ICC with Cisco Nexus Reference Guide* (MK-92HNAS085)—This document describes how to configure Cisco Nexus series switches for use as an ICC (intra-cluster communication) switch.
- *File System Snapshots Operational Best Practice* (MK-92HNAS068)—This document provides operational guidance on file system snapshots.
- *Virtual Infrastructure Integrator for Hitachi Storage Platforms Operational Best Practice* (MK-92HNAS069)—This document provides operational guidance on Hitachi Virtual Infrastructure Integrator for the HNAS platform.
- *Hitachi NAS Platform Replication Best Practices Guide* (MK-92HNAS070)—This document details the best practices for configuring and using HNAS Replication and related features.
- *Hitachi NAS Platform to Hitachi Virtual Storage Platform Unified Gx00 Models Migration Guide* (MK-92HNAS075)—This best practice guide describes how to perform a data-in-place migration of the Hitachi NAS Platform and Virtual Storage Platform (VSP) Gx00 File solution to the VSP Gx00 platform.

## Accessing product documentation

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

## Getting help

The [Hitachi Vantara Support Website](https://support.hitachivantara.com/en_us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: [https://support.hitachivantara.com/en\\_us/contact-us.html](https://support.hitachivantara.com/en_us/contact-us.html).

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

## Comments

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

**Thank you!**



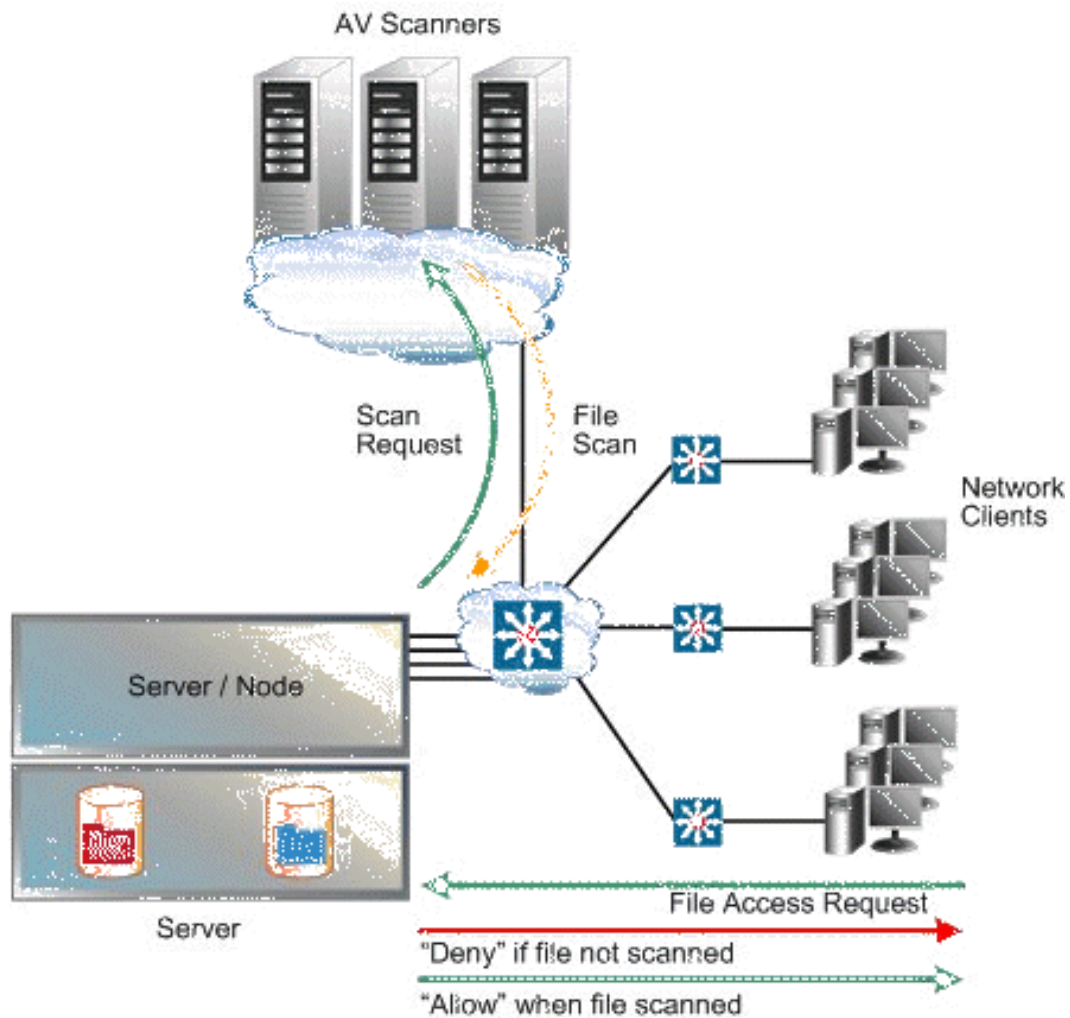
---

## About virus scanning

The storage server architecture reduces the effect of a virus because the file system is hardware-based. This prevents viruses from attaching themselves to (or deleting) system files required for server operation. However, viruses can still propagate and infect user data files that are stored on the server. Therefore, customer support works with industry leading antivirus (AV) software vendors to ensure that the server integrates into an organization's existing AV solutions and without requiring special installations of AV software and servers. To reduce the effect that a virus may have on user data, customer support recommends that AV be configured for the server and that AV software run on all user workstations.

### Virus scanning overview

The server itself does not perform any scanning of the files, but rather provides a connection with configured Virus Scan Engines on the network:



You can configure multiple Virus Scan Engines to enhance both the performance and to maintain high-availability of the server. If a Virus Scan Engine fails during a virus scan, the storage server automatically redirects the scan to another Virus Scan Engine.

The server maintains a list of file types, the Inclusion List, that allows the administrator to control which files are scanned (for example, .exe, .dll, .doc, and so forth). The default Inclusion List includes most file types commonly affected by viruses.

**⚠ Caution:** When virus scanning is enabled, the server must receive notification from a Virus Scan Engine that a file is clean before allowing access to the file. As a result, if virus scanning is enabled and there are no Virus Scan Engines available to service the virus scans, CIFS clients may experience a temporary loss of data access. To ensure maximum accessibility of data, configure multiple Virus Scan Engines to service each EVS on which virus scanning has been enabled.

If virus scanning is temporarily disabled, files continue to be marked as needing to be scanned. In this way, if virus scanning is re-enabled, files that were changed are re-scanned the next time they are accessed by a CIFS client.

The Hitachi NAS platforms storage systems proactively submit files for scanning to the scan engine (SAVSE) on both read (open) and changes and modifications associated with a write (close). If a file has not been verified by a virus scan engine as clean, it will need to be scanned before it can be accessed. However, scanning for viruses when a client is trying to access the file can take time (on read only). To reduce this latency, files are automatically queued to be scanned as soon as they are created or modified, and then closed (on writes). Queued files are scanned promptly, expediting the detection of viruses in new or modified files and making it unlikely that a virus infected file will remain dormant on the system for a long period of time.

Virus Scanning statistics for the storage server (in 10-second time slices) are available for activity since the previous reboot or since the point when statistics were last reset.



**Note:** When a virus is detected, a severe event is placed in the Event Log, identifying the path of the infected file and the IP address of the infected machine. For information on accessing the event log, see the *Server and Cluster Administration Guide*.

You can also set a list of file types on a file system that will be excluded from being sent for scanning by antivirus servers. With an exclusion list you can scan all files except those with certain file extensions, for example, those containing application data. This helps reduce the load on the virus scanning engines and network.

As with the inclusion list, the exclusion list will support wildcarding. The exclusion list is configurable using the command line interface.

## Using the Internet Content Adaption Protocol (ICAP)

The Internet Content Adaption Protocol (ICAP) is an open standard being adopted to connect devices to enterprise-level virus scan engines. ICAP is becoming the preferred means of virus scanning over the previous RPC-based mechanism of virus scanning. RPC is a legacy remote procedure call interface that some scan engines support.

ICAP provides simple object-based content vectoring for HTTP services. ICAP is a protocol for executing a remote procedure call on HTTP messages. It allows ICAP clients to pass HTTP messages to ICAP servers for transformations or other processing (adaptation). The server executes its transformation service on messages and sends back responses to the client, usually with modified messages. Typically, the adapted messages are either HTTP requests or HTTP responses.

ICAP is primarily designed to facilitate the deployment of various value-added services to web serving systems. Inbound and outbound HTTP traffic can be modified by diverting requests or responses through an “ICAP Server”. This server performs content adaptation, such as ad insertion or virus scanning. ICAP is also used in non-web serving environments, such as NAS systems in which client/server protocols have similar requirements for content adaptation. In NAS platforms, ICAP virus scanning cleans file before they are sent. A client requests files, and the NAS platform delegates the task of ensuring these files are clean to external systems, called “scan engines”, before sending them to the client.

The ICAP feature does not require installation. It can be configured using the CLI or SMU. There are no special prerequisites in terms of hardware platform or licenses (ICAP is not a licensed feature). Virus scanning may impact performance when enabled as it adds an overhead when reading files as they are scanned. The performance impact will depend on the number of virus scan engines connected to the system and the dynamic nature of the data on the NAS system.

All virus scan related settings apply at the per-EVS level.

## Configuring virus scan engines

You should configure multiple virus scan engines to enhance performance and high-availability of the server.

You may select between the legacy RPC protocol or the newer ICAP when setting up new virus scan engines.

After installation and configuration has been completed, the virus scan engine will automatically self-register with the server.

## Compatibility with SMB3 Multichannel

If the virus scanner server has multiple network interface cards (NICs) installed, some virus scan engines cannot use SMB3 Multichannel with the NAS server. Check with your NAS server provider for information about compatible virus scan engines when using multiple NICs.

## Enabling virus scanning on the storage server

If virus scanning is enabled and configured for the global context or for the EVS hosting the file system pointed to by the share, then when the share is created, virus scanning is enabled by default. If virus scanning is not enabled for the global context or for the EVS hosting the file system pointed to by the share, then when the share is created, virus scanning is not enabled by default, but you can enable it on a per-EVS basis. To do this, select Enable Virus Scanning on the CIFS Share Details page (Home > File Services > CIFS Shares > CIFS Share Details).

### Procedure

1. Navigate to **Home > Data Protection > Virus Scanning** to display the **Virus Scanning** page.

### Virus Scanning

EVS: g1-eps3 [change...](#)

Mode: RPC

Virus Scanning: Disabled [enable](#)

Scan All File Types

Scan Files With Extensions:

[Add](#)

- ACE
- ACM
- ACV
- ACX
- ADT
- APP
- ASD
- ASP
- ASX
- AVB

[restore defaults](#)

[apply](#)




---

#### Registered Virus Scan Engines

<a href="#">Scan Engine</a>	<a href="#">IP Address</a>	<a href="#">Domain</a>	<a href="#">Status</a>
-----------------------------	----------------------------	------------------------	------------------------

**Actions:** [add](#) [delete](#) [enable](#) [disable](#) | [Request Full Scan](#) [Switch to ICAP mode](#)

**Shortcuts:** [Virus Statistics](#)

Field/Item	Description
EVS	Displays the EVS to which this page applies. Click <b>change</b> to select a different EVS.
Mode	Indicates the virus scan mode.
Virus Scanning	<p>Indicates whether virus scanning is enabled or disabled for the selected EVS. Click <b>enable</b> to enable virus scanning. Virus scanning can be suspended at any time by selecting the <b>disable</b> button. If virus scanning services are resumed later, any file that has changed while virus scanning services were disabled, will be scanned the next time they are accessed by a CIFS client.</p> <p> <b>Tip:</b> Virus scanning can be disabled on individual CIFS shares by clearing the <b>Enable Virus Scanning</b> check box in the <b>Add Shares</b> page (<b>File Services &gt; CIFS Shares &gt; Add Share</b>) or the <b>CIFS Share Details</b> page (<b>File Services &gt; CIFS Shares &gt; CIFS Share Details</b>).</p> <p> <b>Note:</b> For virus scanning to be enabled, it is important that at least one virus scan engine is listed in the <b>Registered Virus Scan Engines</b> table on this page.</p>
Scan All File Types	Scans all file types, regardless of those defined in the <b>File type to scan</b> list.
Scan Files With Extension	<p>Scans specific file types, and ensure that the list of file types contains the appropriate file extensions. The default list includes most files commonly affected by viruses. To add a file type to scan, enter the file extension in the field, and click <b>Add</b>. To delete a file type from the list, select the file type, and click <b>X</b>. To revert to the original list of files to scan, select <b>restore defaults</b>.</p> <p> <b>Note:</b> When you choose to limit the scan to specific file types, only the file types you include in the list are scanned; file types not listed are not scanned.</p>
restore defaults	Restores the file extension list to the default.
<b>apply</b>	Saves any changes.
Registered Virus Scan Engines	Lists the virus scan engines configured for the current EVS.

Field/Item	Description
Scan Engine	The virus scan engine configured for the current EVS.
Port	The port used by the scan engine.
Service Name	Dependent on the scan engine used, for example <b>SYMCScanResp-AV</b> or <b>AVSCANRESP</b> .
Enabled	Whether the scan engine is enabled or disabled.
Status	<ul style="list-style-type: none"> <li>▪ <b>Green:</b> OK: The <b>Scan Engine</b> IP address is valid.</li> <li>▪ <b>Red:</b> Not Responding: an invalid IP address was entered in the <b>Scan Engine</b> field.</li> <li>▪ <b>Grey:</b> Virus scanning is Disabled.</li> </ul>
Actions	<ul style="list-style-type: none"> <li>▪ <b>add</b> opens the Add Scan Engine page.</li> <li>▪ <b>delete</b> deletes the selected virus scan engine.</li> <li>▪ <b>enable</b> enables the selected virus scan engine.</li> <li>▪ <b>disable</b> disables the selected virus scan engine.</li> </ul>
<b>Request Full Scan</b>	Each file is rescanned on next access - even if the file had previously been marked as clean.
<b>Switch to ICAP mode/ Switch to RPC mode</b>	Changes the virus scan mode.

2. Select the **Virtual Server (EVS)** on which to enable virus scanning.



**Caution:** It is important that at least one virus scan engine is listed in the Registered Virus Scanners table. The account used to start the scanning services on the virus scan engine must be added to the server's Backup Operators Local Group. If the account used to start the antivirus service is not a member of the Backup Operators Local Group, the antivirus engine will not be registered and will not be displayed on the **Virus Scanning** page in NAS Manager. If you try to enable virus scanning when no virus scanners have been registered, the SMU restricts the action; virus scanning cannot be enabled when there are no registered virus scanners.

3. Click **enable** next to the Enable Virus Scanning field to enable scanning.  
Virus scanning can be disabled on individual CIFS shares by unchecking the **Enable Virus Scanning** box in the **Add Shares** page (**File Services > CIFS Shares > Add Share**).

4. Optionally, modify the list of files to be scanned:
  - To scan all file types regardless of those in the list, select **Scan All File Types**. It is advisable to select this option while compiling your list of file types to scan.
  - To add a file type to scan, click the **Scan Files With Extensions** radio button, enter the file extension in the field below it, then click **Add**.
  - To delete a file type, select it from the list, and click the **X**.
  - To revert back to the original default list of files types to scan, click **restore defaults**.



**Caution:** The default list of file extensions contains the most commonly used file types. Contact your antivirus software vendor for an up-to-date list of file types that should be included for scanning, and to modify the your file extension list accordingly. It is your responsibility to choose the file types you include for scanning. Based on your needs, the antivirus software used, and the recommendations of the antivirus software manufacturer, choose the file types you want to include in the antivirus scanning; *types not listed will not be scanned*.

The default file extension list is as follows:

ACE, ACM, ACV, ACX, ADT, APP, ASD, ASP, ASX, AVB, AX, BAT, BO, BIN, BTM, CDR, CFM, CHM, CLA, CLASS, CMD, CNV, COM, CPL, CPT, CPY, CSC, CSH, CSS, DAT, DEV, DL, DLL, DOC, DOT, DVB, DRV, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTT, HTW, HTX, IM, INF, INI, JS, JSE, JTD, LIB, LGP, LNK, MB, MDB, MHT, MHTM, MHTML, MOD, MPD, MPP, MPT, MRC, MS, MSG, MSO, MP, NWS, OBD, OBT, OBJ, OBZ, OCX, OFT, OLB, OLE, OTM, OV, PCI, PDB, PDF, PDR, PHP, PIF, PL, PLG, PM, PNF, PNP, POT, PP, PPA, PPS, PPT, PRC, PWZ, QLB, QPW, REG, RTF, SBF, SCR, SCT, SH, SHB, SHS, SHT, SHTML, SHW, SIS, SMM, SWF, SYS, TD0, TLB, TSK, TSP, TT6, VBA, VBE, VBS, VBX, VOM, VS?, VSD, VSS, VST, VWP, VXD, VXE, WBT, WBK, WIZ, WK?, WML, WPC, WPD, WS?, WSC, WSF, WSH, XL?, XML, XTP, 386

5. If a virus scanner has been disabled for some reason, you can re-enable its usage by filling the check box next to the name of the disabled virus scanner and clicking the **enable** button in the **Actions** area.
6. Verify your settings, and click **apply** to save.

## Forcing files to be rescanned

With the appearance of a new virus and release of antivirus software updates, it is important to rescan all files, including those that have not changed since the last time they were scanned.

### Before you begin

Be aware that rescanning migrated files increases file recall times for users (recall time + scan time) the first time each file is accessed.



**Procedure**

1. Navigate to **Home > Data Protection > Virus Scanning** to display the **Virus Scanning** page.
2. Click the **Request Full Scan** link.

This marks every file as unscanned, so the file will be scanned the next time it is accessed.

## Enabling an exclusion list

You can enable an exclusion list using CLI commands.

Use this procedure to enable an exclusion list of file types that will be excluded from scanning by antivirus servers.

**Before you begin**

Note that the management of an exclusion list is on a per-EVS basis.

**Procedure**

1. Add file types to the exclusion list by using `virusscan-exclusion-list-add` CLI command.

```
virusscan-exclusion-list-add BAT,COM,DOC,EXE,PPT
```

There must be no whitespace between consecutive types. 250 entries can be added to the exclusion list.

2. Enable the exclusion list by using the `virusscan-exclusion-list-enable` command.

```
virusscan-exclusion-list-enable
```

File types can also be removed, and the list can be disabled and cleared. See the man pages for:

- `virusscan-exclusion-list-remove`
- `virusscan-exclusion-list-disable`
- `virusscan-exclusion-list-clear`

**Related task**

[Enabling virus scanning on the storage server \(on page 12\).](#)

## Enabling maximum file size for virus scanning

With release 12.5 and later, you can enable a maximum file size using CLI commands.

Use this procedure to enable the maximum file size setting, so that files above that size will be excluded from scanning by antivirus servers.

**Before you begin**

Note that the management of the maximum file size setting is on a per-EVS basis.

Relationship with inclusion/exclusion lists:

- If the inclusion list is used, the file must be of a type in the inclusion list.
- If the exclusion list is used, the file type must not be in the exclusion list.

### Procedure

1. The maximum file size setting is disabled by default. Set the value to be used for the maximum file size setting before enabling the maximum file size.

The default value is 1 MB. The maximum file size setting can be set using numeric values with a unit (B, KB, MB, GB, KiB, MiB, GiB). If there is no unit, it is assumed to be Bytes (B). The maximum value you may use for this setting is 15 EiB.

```
virusscan-max-file-size-set <size>
```

2. Enable the maximum file size setting.  
**virusscan-max-file-size-enable**
3. Check the state of the maximum file size setting and its current value.  
**virusscan-max-file-size-show**
4. If you want to disable the maximum file size setting:  
**virusscan-max-file-size-disable**

**Hitachi Vantara**



Corporate Headquarters  
2535 Augustine Drive  
Santa Clara, CA 95054 USA  
[HitachiVantara.com](http://HitachiVantara.com) | [community.HitachiVantara.com](http://community.HitachiVantara.com)

Contact Information  
USA: 1-800-446-0744  
Global: 1-858-547-4526  
[HitachiVantara.com/contact](http://HitachiVantara.com/contact)