Configuring Symantec™ Protection Engine for Network Attached Storage 7.0 for the IBM SONAS and Storwize V7000 Unified systems
Configuring Symantec™ Protection Engine for Network Attached Storage 7.0 for the IBM SONAS and Storwize V7000 Unified systems

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 7.0

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan               customercare_apac@symantec.com
Europe, Middle-East, and Africa      semea@symantec.com
North America and Latin America     supportsolutions@symantec.com
Configuring Symantec™ Protection Engine for Network Attached Storage 7.0 for the IBM SONAS and Storwize V7000 Unified systems

This document includes the following topics:

■ About software components
■ How Symantec Protection Engine works with the IBM SONAS and Storwize V7000 Unified systems
■ About specifying which file types are scanned
■ About specifying the scan policy
■ About preparing for installation
■ Configuring the ICAP-specific options
■ Scheduling LiveUpdate to update virus definitions automatically
■ Configuring Rapid Release updates to occur automatically
■ About configuring the IBM SONAS and Storwize V7000 Unified systems
About software components

Symantec™ Protection Engine for Network Attached Storage (NAS) provides virus scanning and repair capabilities for the IBM SONAS and Storwize V7000 Unified systems.

Symantec Protection Engine for Network Attached Storage is hereafter referred to as Symantec Protection Engine.

The IBM SONAS and Storwize V7000 Unified systems support antivirus solutions from Symantec that are installed, configured, maintained, and operated by the customer. The IBM SONAS and Storwize V7000 Unified systems configuration options control the actions taken by these systems, either before or after submitting a request to Symantec Protection Engine to scan a file, while the Symantec Protection Engine configuration options independently control the actions taken by Symantec Protection Engine during the process of scanning the file. Therefore, both the IBM SONAS and Storwize V7000 Unified systems and Symantec Protection Engine must each be configured appropriately for an option to operate as intended.

To use antivirus scanning with the IBM SONAS and Storwize V7000 Unified systems, configure Symantec Protection Engine to provide virus scanning and repair services. For more information, see the Symantec Protection Engine for Network Attached Storage Implementation Guide.

Virus scanning is an integral part of the IBM SONAS and Storwize V7000 Unified systems starting with IBM SONAS version 1.2 and 1.3 and Storwize V7000 Unified systems version 1.3 and 1.4. No separate code installation or license is required.

See “About configuring the IBM SONAS and Storwize V7000 Unified systems” on page 20.
SONAS and Storwize V7000 Unified systems using the Common Internet File System (CIFS) protocol.

Internet Content Adaptation Protocol (ICAP) is used to communicate with Symantec Protection Engine. For load balancing, you can configure a pool of protection engines. The IBM Storwize V7000 Unified systems selects a protection engine from the pool list at scan time. If a protection engine cannot be reached, it is temporarily removed from the pool of available protection engines. In this case, the IBM SONAS and Storwize V7000 Unified systems select a different protection engine that is available from the pool, and periodically attempts to reinstate the removed protection engine.

How files are scanned

The IBM SONAS and Storwize V7000 Unified systems initiate the scan of a file in real time when a file is opened. The IBM SONAS and Storwize V7000 Unified systems can optionally be configured to scan a file in real time when the file is closed, if the file has been modified. You can also define and submit on-demand scans, and configure scheduled bulk scans.

When a user attempts to access a file from the IBM SONAS and Storwize V7000 Unified systems, these systems open a connection with Symantec Protection Engine. The IBM SONAS and Storwize V7000 Unified systems then pass the file to the protection engine for scanning. When scanning is complete, the IBM SONAS and Storwize V7000 Unified systems close the connection with the protection engine.

Symantec Protection Engine indicates the scanning results to the IBM SONAS and Storwize V7000 Unified systems after a file is scanned. The protection engine also returns the repaired file if the file is infected and can be repaired.

After the IBM SONAS and Storwize V7000 Unified systems receive the scanning results, the file is handled in the following manner:

Only clean files are passed to the requesting user. If a file is infected and can be repaired, the repaired file is passed to the requesting user. The stored version of the infected file is replaced with the repaired file. Parameters can be set to control whether to deny access to a file if scanning is not possible at the time, when a virus is detected and repair is not possible, or whether to quarantine or delete the file. A permission denied type of error notifies the end user attempting to access an unrecoverable file. Optionally, the path by which the file was opened for the current scan can be moved to a subdirectory created for that purpose and accessible only by the root user.
How caching works

The time stamp of a scan and the antivirus definition file signature are saved as extended attributes for each file scanned. Cached antivirus scan information is checked when a file is opened to determine whether a file must be scanned. After an update of a virus definition, which provides a new signature, each file must be rescanned before it can be read again. A bulk rescan can be initiated on demand to run asynchronously to proactively rescan files during a convenient time window rather than waiting for the next read of each file. The IBM SONAS and Storwize V7000 Unified systems cache the scanning results for each clean file. The cached information includes the date and revision number of the virus definitions that were used to perform the scan. So, if a second user requests access to a file that has already been scanned, and the virus definitions have not changed, a redundant scan is avoided.

About specifying which file types are scanned

You must configure settings on both, the IBM SONAS and Storwize V7000 Unified systems and Symantec Protection Engine in order to specify the file types to be scanned for viruses.

About specifying file types on the IBM SONAS and Storwize V7000 Unified systems

Based on file extensions, the IBM SONAS and Storwize V7000 Unified systems initially determine whether it should pass a file to Symantec Protection Engine for scanning. You can control which files are scanned by using an exclusion or an inclusion list, or you can scan all files regardless of the extension. The IBM SONAS and Storwize V7000 Unified systems antivirus parameters can be set at the export, file system, file set, or path level to specify which file extensions to include in, or exclude from a scan. Include those file extensions in the exclusion list if they are not likely to contain viruses.

If the include list is empty or not specified, the default is that all extensions are scanned. In this case, the exclude list can be used to create exceptions.

See “About configuring virus scanning on the IBM SONAS and Storwize V7000 Unified systems” on page 21.

About specifying file types on Symantec Protection Engine

You can configure Symantec Protection Engine to exclude selected file types and file extensions from being scanned. The settings on Symantec Protection Engine are as important as the settings on the IBM SONAS and Storwize V7000 Unified systems.
systems. The settings on the protection engine determine which files to scan upon receiving a file from the IBM SONAS and Storwize V7000 Unified systems. The scanned files are those contained in archive or container file formats. You can control which embedded files are scanned by using the file type and extension exclusion list, or you can scan all files regardless of extension.

**Note:** Exclusion lists ensure that all file types are not scanned. Therefore, new types of viruses might not be detected. Scanning all files regardless of extension and type is the most secure setting, but it imposes the heaviest demand on resources. During virus outbreaks, you must scan all files even if you normally control the file types that are scanned with the exclusion list.

For more information, see the *Symantec Protection Engine for Network Attached Storage Implementation Guide*.

See “About specifying the file types to scan on Symantec Protection Engine” on page 11.

### About specifying the file types to scan on Symantec Protection Engine

The settings on Symantec Protection Engine must be configured to specify the types of files to be scanned for viruses. This setting on the protection engine determines which files to scan on receiving a file from the IBM SONAS and Storwize V7000 Unified systems. The scanned files are those contained in archive or container file formats.

You can control which embedded files are scanned by using an exclusion list, or you can scan all files regardless of extension and type. A prepopulated exclusion list of file types and file extensions exist for you to modify. The Symantec Protection Engine is configured by default to scan all files.

**Note:** Symantec Protection Engine examines the first few bytes of every file to determine whether the file could contain a virus. This action occurs even if the file extension is not one that was identified for scanning. Based on this examination, the protection engine may scan a file even though it has not been identified for scanning.

For more information, see the *Symantec Protection Engine for Network Attached Storage Implementation Guide*.

See “About configuring virus scanning on the IBM SONAS and Storwize V7000 Unified systems” on page 21.
Specifying which file types to scan

You can control which file types are scanned by specifying those extensions that you want to exclude from scanning, or you can scan all files regardless of extension.

**To scan all files except for those that are in the file extension exclusion list**

1. On the Symantec Protection Engine administrative interface, in the left pane, click *Policies*.
2. Under Views, click *Scanning*.
3. In the right pane, under *Files to Scan*, click *Scan all files except those in the extension or type exclude lists*.

   When you enable this option, both the file extension exclude list and the file type exclude list are activated automatically.
4. Enter the file extension that you want to add to the list on a separate line. Use a period with each extension in the list.
5. To remove a file extension from the list, select it and delete it from the *File extension exclude* list.
6. To restore the default file extension exclude list, in the left pane, under *Tasks*, click *Reset Default List*.
7. On the toolbar, select one of the following:

   **Save**
   - Saves your changes.
   - You can continue to make changes in the administrative interface until you are ready to apply them.

   **Apply**
   - Applies your changes.
   - Your changes are not implemented until you apply them.

**To scan all file types except for those in the file type exclusion list**

1. On the Symantec Protection Engine administrative interface, in the left pane, click *Policies*.
2. Under Views, click *Scanning*.
3. In the right pane, under *Files to Scan*, click *Scan all files except those in the extension or type exclude lists*. When you enable this option, both the file type exclude list and the file extension exclude list are activated automatically.
4 Enter the file type that you want to add to the list on a separate line.
   To include all subtypes for a file type, use the wildcard character /*. For more information on how to write the file types, see the Symantec Protection Engine for Network Attached Storage Implementation Guide.

5 To remove a file type from the list, select it and delete it from the File type exclude list.

6 To restore the default file type exclude list, in the left pane, under Tasks, click Reset Default List.

7 On the toolbar, select one of the following:

   Save
   Saves your changes.
   You can continue to make changes in the administrative interface until you are ready to apply them.

   Apply
   Applies your changes.
   Your changes are not implemented until you apply them.

To scan all files regardless of extension or type

1 On the Symantec Protection Engine administrative interface, in the left pane, click Policies.

2 Under Views, click Scanning.

3 In the right pane, under Files to Scan, click Scan all files.

4 On the toolbar, select one of the following:

   Save
   Saves your changes.
   You can continue to make changes in the administrative interface until you are ready to apply them.

   Apply
   Applies your changes.
   Your changes are not implemented until you apply them.
About specifying container handling limits

File attachments that consist of container files can overload the system and cause denial-of-service attacks. They can be overly large, contain a large number of embedded or compressed files, or be designed to maliciously use resources and degrade performance. Symantec Protection Engine can be configured to impose limits on how container files are handled. This reduces the exposure of the network to denial-of-service attacks.

You can specify the following limits for handling container files:

- The maximum amount of time, in seconds, that is spent decomposing a container file and its contents. This setting does not apply to .hqx or .amg files.
- The maximum file size, in megabytes, for the individual files that are in a container file.
- The maximum number of nested levels to decompose for scanning.
- The maximum number of bytes that are read when determining whether a file is MIME encoded.

You can specify whether to allow or deny access to the file if any of these specified limits are met or exceeded.

Symantec Protection Engine blocks container files based on their type, because only certain file types contain virus or malicious code. You can configure Symantec Protection Engine to block partial container files, malformed container files, and encrypted container files as well.

For more information on container handling limits, see the *Symantec Protection Engine for Network Attached Storage Implementation Guide*.

About specifying the scan policy

You configure the scan policy through the Symantec Protection Engine administrative interface. The protection engine can be configured to do any of the following:

- **Scan only**
  - Scan files for viruses. No action taken on infected files.

- **Scan and delete**
  - Scan files for viruses. Delete infected files that are embedded in archive or container files without trying to repair.
Scan and repair files  
Scan files for viruses. Try to repair infected files. No action taken on unrepairable files (that is, unrepairable files are not deleted from archive or container files).

Scan and repair or delete  
Scan files for viruses. Try to repair infected files. Delete unrepairable files from archive or container files.

About handling infected files on the IBM SONAS and Storwize V7000 Unified systems

When an unrepairable infected file is found, optional parameters at the export, file system, file set, and path level specify whether to quarantine or delete the file. Optionally, the path by which the file was opened for the current scan can be moved to a subdirectory created for that purpose and accessible only by the root user.

For more information, see the appropriate IBM SONAS and Storwize V7000 Unified systems documentation.

About preparing for installation

The computer on which you plan to install Symantec Protection Engine must meet the system requirements that are listed in the *Symantec Protection Engine for Network Attached Storage Implementation Guide*.

After you have installed Symantec Protection Engine, configure the virus scanning functionality on the IBM SONAS and Storwize V7000 Unified systems.

About configuring Symantec Protection Engine

You must configure several settings on each Symantec Protection Engine that is used to support scanning for the IBM SONAS and Storwize V7000 Unified systems.

**Note:** The configuration settings on each protection engine must be identical if you are using multiple protection engines to support scanning for an IBM SONAS or Storwize V7000 Unified system. LiveUpdate and Rapid Release should be scheduled to occur at the same time on all protection engines so that the virus definitions are consistent at all times.
The protection engine must be configured to use ICAP as the communication protocol. ICAP is the default protocol at installation. After you have selected ICAP, you must configure the ICAP-specific options.

**Configuring the ICAP-specific options**

After you install Symantec Protection Engine, you must configure several settings that are specific to the ICAP protocol through the Symantec Protection Engine administrative interface. If Symantec Protection Engine has already been configured to use another protocol, you can change the protocol through the administrative interface. However, you must manually restart Symantec Protection Engine.

For more information about accessing the administrative interface, see the *Symantec Protection Engine for Network Attached Storage Implementation Guide.*

Table 1-1 describes the protocol-specific options for ICAP.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind address</td>
<td>Symantec Protection Engine detects all of the available IP addresses that are installed on the host. By default, Symantec Protection Engine accepts scanning requests on (binds to) all of the scanning IP addresses that it detects. You can configure up to 64 IP addresses as the scanning IP addresses. You can specify whether you want Symantec Protection Engine to bind to all of the IP addresses that it detects, or you can restrict access to one or more interfaces. If you do not specify at least one IP address, Symantec Protection Engine binds to all of the scanning IP addresses that it detects. If Symantec Protection Engine fails to bind to any of the selected IP addresses, an event is written to the log as a critical error. You can access the console even if Symantec Protection Engine is unable to bind to any IP address, however, scanning functionality is unavailable.</td>
</tr>
<tr>
<td>Port number</td>
<td>The port number must be exclusive to Symantec Protection Engine. For ICAP, the default port number is 1344. If you want to change the port number, use a number greater than 1024 that is not in use by any other program or service.</td>
</tr>
</tbody>
</table>
Table 1-1  ICAP-specific options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan policy</td>
<td>Symantec Protection Engine can be configured to do any of the following:</td>
</tr>
<tr>
<td></td>
<td>■ Scan only: Scan files for viruses. No action taken on infected files.</td>
</tr>
<tr>
<td></td>
<td>■ Scan and delete: Scan files for viruses. Delete any infected files that are embedded in archive or container files without trying to repair them.</td>
</tr>
<tr>
<td></td>
<td>■ Scan and repair files: Scan files for viruses. Try to repair infected files. No action taken on unrepairable files (that is, do not delete the files from archive or container files).</td>
</tr>
<tr>
<td></td>
<td>■ Scan and repair or delete: Scan files for viruses. Try to repair infected files. Delete unrepairable files from archive or container files.</td>
</tr>
</tbody>
</table>

To configure ICAP-specific options

1. On the Symantec Protection Engine administrative interface, in the left pane, click **Configuration**.

2. Under Views, click **Protocol**.

3. In the right pane, under Select Communication Protocol, click **ICAP**.

   The configuration settings are displayed for the selected protocol. If you change the protocol setting from RPC to ICAP through the Symantec Protection Engine administrative interface, you must manually stop and restart the service.

4. Under ICAP Configuration, in the **Bind** address box, select the scanning IP addresses that you want to bind to Symantec Protection Engine. Select the **Select All** check box to select every IP Address in the **Bind** address table.

   By default, Symantec Protection Engine binds to all interfaces.

5. In the **Port number** box, enter the TCP/IP port number that the IBM SONAS and Storwize V7000 Unified systems use to pass files to Symantec Protection Engine for scanning.

   The default setting for ICAP is port 1344.
In the Scan policy list, select how you want Symantec Protection Engine to handle infected files. The default setting is **Scan and repair or delete**, which is the recommended setting.

On the toolbar, select one of the following:

- **Save** saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
- **Apply** applies your changes. Your changes are not implemented until you apply them.

---

**Scheduling LiveUpdate to update virus definitions automatically**

Scheduling LiveUpdate to occur automatically at a specified time interval ensures that Symantec Protection Engine always has the most current virus definitions. If you use multiple protection engines to support virus scanning, schedule LiveUpdate to occur at the same time for each protection engine. This scheduling ensures that all protection engines have the same version of virus definitions. Having the same version of virus definitions is necessary for proper functioning of virus scanning on the IBM SONAS and Storwize V7000 Unified systems.

You must schedule LiveUpdate on each Symantec Protection Engine. When LiveUpdate is scheduled, LiveUpdate runs at the specified time interval relative to the LiveUpdate base time. The default LiveUpdate base time is the time at which the protection engine was installed.

You can change the LiveUpdate base time. If you change the scheduled LiveUpdate interval, the interval adjusts based on the LiveUpdate base time.

For more information on changing the base time, see the *Symantec Protection Engine for Network Attached Storage Implementation Guide*.

**To schedule LiveUpdate to update virus definitions automatically**

1. On the Symantec Protection Engine administrative interface, in the left pane, click **System**.
2. Under **Views**, click **LiveUpdate Content**.
3 In the right pane, under LiveUpdate Content, select the Enable scheduled LiveUpdate check box.
This option is enabled by default.

4 In the LiveUpdate interval drop-down list, select an interval.
You can select from 2, 4, 8, 10, 12, or 24-hour intervals. The default LiveUpdate interval is 2 hours.

5 On the toolbar, select one of the following:

- **Save**
  Saves your changes.
  You can continue to make changes in the administrative interface until you are ready to apply them.

- **Apply**
  Applies your changes.
  Your changes are not implemented until you apply them.

### Configuring Rapid Release updates to occur automatically

You can configure Symantec Protection Engine to obtain uncertified definition updates with Rapid Release. You can also configure Symantec Protection Engine to retrieve Rapid Release definitions every 5 minutes to every 120 minutes.

The Rapid Release definitions are created when a new threat is discovered. These definitions undergo basic quality assurance tests by Symantec Security Response. However, they do not undergo the intense testing that is required for a LiveUpdate release. Symantec updates the Rapid Release definitions, as needed, to respond to high-level outbreaks.

---

**Warning:** Rapid Release definitions do not undergo the same rigorous quality assurance tests as LiveUpdate and Intelligent Updater definitions. You must rely on the full quality-assurance-tested definitions whenever possible. Ensure that you deploy Rapid Release definitions to a test environment before you install them on your network.

If you use a proxy or firewall that blocks FTP communications, the Rapid Release feature does not function. Your environment must allow FTP traffic for the FTP session to succeed.
You can schedule the Rapid Release updates to occur automatically at a specified time interval to ensure that Symantec Protection Engine always has the most current definitions. Scheduled Rapid Release updates are disabled by default.

**To configure Rapid Release updates to occur automatically**

1. On the Symantec Protection Engine administrative interface, in the left pane, click **System**.
2. Under **Views**, click **Rapid Release Content**.
3. In the content area under Rapid Release Content, select the **Enable scheduled Rapid Release** check box to enable automatic downloads of Rapid Release definitions.
   This option is disabled by default.
4. In the Rapid Release interval box, select any number between 5 minutes and 120 minutes to specify the interval between which you want Symantec Protection Engine to download Rapid Release definitions. The default value is 30 minutes.
5. On the toolbar, select one of the following:
   - **Save**: Saves your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - **Apply**: Applies your changes. Your changes are not implemented until you apply them.

---

**About configuring the IBM SONAS and Storwize V7000 Unified systems**

You must register at least one Symantec Protection Engine for each IBM SONAS and Storwize V7000 Unified system for which you provide virus scanning. You also must configure the virus scan functionality in accordance with the IBM SONAS and Storwize V7000 Unified systems documentation.

For more information, see the appropriate IBM SONAS and Storwize V7000 Unified systems documentation.
About configuring virus scanning on the IBM SONAS and Storwize V7000 Unified systems

You must configure virus scanning for each IBM SONAS and Storwize V7000 Unified system. The IBM SONAS and Storwize V7000 Unified systems Command Line Interface (CLI) is used for configuring and displaying IBM SONAS and Storwize V7000 Unified systems antivirus parameters. The CLI is also used for starting and stopping bulk scans or for viewing bulk scan status. The IBM SONAS and Storwize V7000 Unified systems antivirus configuration can be changed dynamically and does not require shutdown or restart.

**Note:** The virus scan functionality for each IBM SONAS and Storwize V7000 Unified system that is accessing a protection engine must be identically configured to avoid inconsistency. The scan results and repair results for infected files will be inconsistent if the settings differ among IBM SONAS and Storwize V7000 Unified systems using the same protection engine.

The `cfgav` command is used to configure virus scanning on the IBM SONAS and Storwize V7000 Unified systems and operates on a scope. A scope is a subtree of the file namespace identified by the path to the root of the subtree, such that all file accesses within that subtree share a set of antivirus settings. You can specify the scope by using the `--fsys`, `--fset`, `--export`, or `--path` options for a file system, file set, export, or path respectively. The argument to each scope option is a space-separated list, and you can specify multiple scopes within a single `cfgav` CLI command by repeating these options multiple times in any combination. Local parameters specified for an export, file set, or file system are translated to the corresponding file namespace path and not the actual object used to identify the scope, because the association of a file namespace path to an IBM SONAS and Storwize V7000 Unified system object is not unique. For example, multiple exports can refer to the same file namespace path, and an export can refer to the same file namespace path as a file set or a file system.

If no settings are specified for a scope, the settings for the closest enclosing scope are used. When a configuration parameter is initially set for a particular scope, the unspecified settings for the new scope are copied from the closest enclosing scope. Subsequent updates to scopes are completely independent of each other so that changing the setting of a scope does not affect the settings of either its enclosed or enclosing scopes. You can explicitly apply the settings of an enclosing scope to an enclosed scope by using the `--force` option of the `cfgav` command. Alternatively, you can use the `--erase` option of the `cfgav` command to restore the settings of an enclosed scope to the settings of an enclosing scope.
Use the --scan and --noscan options to respectively enable or disable scanning for a specified scope.

To create an include list, add an extension to, or remove an extension from an include list, use the cfgav command with the --set-include, --add-include and --rem-include options, respectively. To create an exclude list, add an extension to, or remove an extension from an exclude list, use the cfgav command with the --set-exclude, --add-exclude and --rem-exclude options respectively.

You can use the --onwrite and --noonwrite options respectively, to enable or to disable scanning when a protected file is written. You can use the --denyonerror and --nodenyonerror options respectively, to deny or to allow users’ access to files that cannot be scanned at file open.

You can use the --qdel and --noqdel options respectively, to enable or to disable file deletion as the action to be taken when a file is determined to be compromised. You can use the --qmove and --noqmove options respectively, to enable or to disable moving a file to the quarantine subdirectory as the action to be taken when a file is determined to be compromised.

When a virus signature is updated, a protected file must be rescanned before it is opened. This could result in significant performance degradation during normal use of the IBM SONAS and Storwize V7000 Unified systems subsequent to a signature update. The bulk scan feature allows an administrator to rescan files after antivirus signatures have been updated during a convenient time window in order to minimize IBM SONAS and Storwize V7000 Unified systems performance issues. A bulk scan performs antivirus scanning of files in the background after a virus signature update without waiting for an application to open a file to perform a scan. Use the IBM SONAS and Storwize V7000 Unified systems CLI ctlaVbulk command to submit a bulk scan, stop a bulk scan or display the status of a bulk scan. To schedule a bulk scan, use the mktask command and specify CtlAvBulk as the task name. On demand and scheduled bulk scans use the same customer supplied external protection engines, IBM SONAS and Storwize V7000 Unified systems interface nodes, and configuration settings before a file is opened. A bulk scan can be submitted on any subset of IBM SONAS and Storwize V7000 Unified systems interface nodes, and multiple processes for a single bulk scan can be submitted to run simultaneously on each node subject to the limits of I/O capacity, network capacity, and scan node capacity. If no scope is specified, by default a bulk scan examines all protected files. You can specify the --fsys, --fset, --export, and --path options to limit the bulk scan scope. Each bulk scan runs simultaneously on all interface nodes that have a normal status. Multiple simultaneous instances of a bulk scan can run against the same file system, in which case the instances are coordinated to avoid scanning the same file more than once. Use the --processes option to specify how many instances of a bulk scan should be run simultaneously.
scan process you want to run on an interface node. If the `--processes` option is not specified, the default is one process for each interface node.

All significant antivirus events are documented in the syslog that is viewable using the IBM SONAS and Storwize V7000 Unified systems Graphical User Interface (GUI). Important antivirus events are also displayed in the alert log. The default basic level information logging includes startup and shutdown as well as periodic performance summary data.

The default log level includes brief startup and shutdown notification entries, periodic one-line performance summaries that can be used to create performance models and to assess performance, and a one-line entry each time a protection engine updates a virus signature that requires files to be rescanned on a subsequent open.

The impact of antivirus scanning on the file access latency of the IBM SONAS and Storwize V7000 Unified systems depends on the following factors:

- Number of registered protection engines
- Symantec Protection Engine CPU performance
- Customer IP bandwidth
- Workload mix including file sizes and read/write ratios
- Content of files to be scanned
- Files and file types to be scanned
- Efficiency caching the scan results

**Note:** Because scan results are invalidated whenever the antivirus vendor updates signatures, the frequency of virus signature updates could also have a significant impact on performance.

You can use the IBM SONAS and Storwize V7000 Unified systems GUI to manage the antivirus by navigating to **Files > Services > Antivirus.**

**Note:** The IBM Storwize V7000 Unified systems management GUI does not support the creation of non-CIFS scheduled bulk scans (for example, mktask or ctlavbulk). When managing antivirus scans using the GUI, only on-access scans are available for files that are exported using a protocol other than CIFS.
Registering Symantec Protection Engine

You must register at least one Symantec Protection Engine to provide the virus scanning for each IBM SONAS and Storwize V7000 Unified system. In a typical environment, a minimum of two protection engines are recommended for increased availability and load balancing. Having one protection engine can cause denial-of-file access, if it does not respond. Multiple protection engines are supported per IBM SONAS and Storwize V7000 Unified system. The IBM SONAS and Storwize V7000 Unified systems handle load balancing across multiple protection engines automatically.

**Note:** You are not required to register the same protection engines for every IBM SONAS and Storwize V7000 Unified system. You can register different protection engines to different IBM SONAS and Storwize V7000 Unified systems. However, all of the protection engines registered with a particular IBM SONAS and Storwize V7000 Unified system must have identical configurations.

You must register Symantec Protection Engine through the `--addscanne` option of the IBM SONAS and Storwize V7000 Unified systems CLI `cfgav` command. For each protection engine that is used for scanning, you must provide the IP address and the port number. You can optionally use the `--timeout` option to set the timeout value in seconds for a scan node response. The default value is 10 seconds. The port number must match the port number that was selected during the installation of Symantec Protection Engine.

Recommendations while integrating multiple Symantec Protection Engines

Do the following when multiple protection engines are used to support a particular IBM SONAS and Storwize V7000 Unified system:

- Configure the settings on each Symantec Protection Engine to be identical.
- Schedule LiveUpdate and Rapid Release to occur at the same time on all of the protection engines that are used by a particular IBM SONAS and Storwize V7000 Unified system. This ensures that the virus definitions are consistent.
- Configure the virus scan functionality to be identical for each IBM SONAS and Storwize V7000 Unified system that uses a particular protection engine to avoid inconsistency. The scan results and repair results for infected files will be inconsistent if the settings differ among IBM SONAS and Storwize V7000 Unified systems using the same protection engine.