# Configuring Symantec™ Protection Engine for Network Attached Storage 8.0 for Hitachi Unified and NAS Platforms

# Configuring Symantec™ Protection Engine for Network Attached Storage 8.0 for Hitachi Unified and NAS Platforms

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.

## Legal Notice



Symantec Corporation 350 Ellis Street Mountain View, CA 94043

https://www.symantec.com

# Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

# Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

# Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Chapter 1

# Configuring Symantec™ Protection Engine for Network Attached Storage 8.0 for Hitachi Unified and NAS Platforms

This chapter includes the following topics:



## About software components

Symantec™ Protection Engine for Network Attached Storage provides virus s canning and repair capabilities for the Hitachi Unified and NAS Platforms.

Configure the following components to add antivirus scanning to the Hitachi NAS devices:

- Symantec™ Protection Engine for Network Attached Storage version 8.0 provides the virus scanning and repair services.

  For more information, see Online Help (UHS) or Implementation Guide for Symantec Protection Engine 8.0.

- Hitachi Unified and NAS Platforms operating on HNAS OS version 13.0 or later. Some options are configured directly on the NAS device. No additional code is necessary to connect Symantec™ Protection Engine for Network Attached Storage to the device.
  - Hitachi VSP N400
  - Hitachi VSP N600

- Hitachi VSP N800

**Note:** Symantec™ Protection Engine for Network Attached Storage is hereafter referred to as Symantec Protection Engine.

## Installing Symantec Protection Engine

The computer on which you plan to install Symantec Protection Engine must meet the system requirements.

See the System requirements topic in Online Help (UHS) or Implementation Guide.

After you have installed Symantec Protection Engine, configure the virus scanning functionality on Hitachi HNAS.

## About the centralized cloud console

Symantec Protection Engine 8.0 introduces the centralized console along with the existing web-based interface, where you can manage multiple Symantec Protection Engine installations. You can manage scanners and scan policies, create assets and alerts, and view the dashboards and events on the centralized console.

You can initialize the on-boarding process to centralized console by using the cloud management utility **cloudmgmtutil** that is available in the installation directory.

After the on-boarding process is complete, you must enroll all your Symantec Protection Engine scanners that you want to manage from the centralized console.

For more information, and to get started with the centralized console, see Quick-start Checklist topic in Online Help (UHS).

See Onboarding to a centralized cloud console

See Video - Onboarding and scanner enrollment

## How Symantec Protection Engine works with the Hitachi Unified and NAS Platforms

Symantec Protection Engine provides virus scanning and repair capabilities for the Hitachi Unified and NAS Platforms that support HNAS OS version 13.0 or later. Virus scanning and repair are provided for files on the Common Internet File System (CIFS).

Internet Content Adaptation Protocol (ICAP) is used to communicate with Symantec Protection Engine. In a typical NAS environment, a minimum of two protection engines are required to handle the scan volume.

A maximum of 32 protection engines can be supported per NAS device. The NAS service handles load balancing across multiple protection engines automatically.

## How are files scanned

The Hitachi NAS device is configured to scan a file in real time (that is, when a file is opened and when it is closed, if it has been modified). When a user tries to access a file from storage, the NAS device opens a connection with Symantec Protection Engine. The device then passes the file to the protection engine for scanning. After scanning is complete, the device closes the connection with the protection engine.

Symantec Protection Engine indicates the scanning result to the NAS device after a file is scanned. After the device receives the scanning results, the file is handled in the following way: Only clean files are passed to the requesting user. If the file is infected, the user is allowed access to the file, denied access to the file, or the file is deleted. User can configure these options on the Hitachi NAS device. The infected file is deleted by default.

## How caching works

The NAS device caches 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 if the virus definitions have not changed, a redundant scan is avoided.

The cache is purged when the virus definitions on Symantec Protection Engine are updated and when the Hitachi NAS device is restarted. Individual cache entries are updated whenever a stored file is changed.

# Configuring Symantec Protection Engine

You must configure several settings on each Symantec Protection Engine that is used to support scanning for the Hitachi NAS device.

**Note:** If you use multiple protection engines to support scanning, the configuration settings on each protection engine must be identical. LiveUpdate must schedule to occur at the same time on all protection engines so that 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

If you select ICAP, you must configure certain options specific to ICAP protocol. You must also configure the ICAP client to work with Symantec Protection Engine.

For more information, see the Implementation Guide or Online Help (UHS).

Protocol-specific options for ICAP describes the protocol-specific options for ICAP.

**Table 2-1 Protocol-specific options for ICAP**

| Option | Description |
|---|---|
| Bind address | Symantec Protection Engine detects all 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 scanning IP addresses.<br><br>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.<br><br>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. Even if Symantec Protection Engine is unable to bind to any IP address, you can access the console. However, scanning functionality is unavailable.<br><br>**Note:** You can use 127.0.0.1 (the loopback interface) to let only the clients that are running on the same computer connect to Symantec Protection Engine. |
| Port number | The port number must be exclusive to Symantec Protection Engine. For ICAP, the default port number is 1344. If you change the port number, use a number greater than 1024 that is not in use by any other program or service. |

### To configure the 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 start 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. Check **Select All** 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, type the TCP/IP port number that the NAS service uses to pass files to Symantec Protection Engine for scanning. The default setting for ICAP is port 1344.
6. 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.
7. On the toolbar, select one of the following:
   - Click **Save** to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click **Apply** to apply your changes. Your changes are not implemented until you apply them.

## About specifying which file types to scan on the protection engine

The settings on Symantec Protection Engine must be configured to specify the types of files to be scanned for viruses. The scan policy on the protection engine determines which files it should scan from the NAS device. The scanned files are those contained in archive or container file formats.

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

For more information, see the Implementation Guide or Online Help (UHS).

### 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. Type each 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**.

   This option restores the default file-type exclude list and the file-extension exclude list.

7. On the toolbar, select one of the following:

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

### To scan all file types except 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. Type each file type 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 Implementation Guide or Online Help (UHS).

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**.

   This option restores the default file-type exclude list and the file-extension exclude list.

7. On the toolbar, select one of the following:

   - Click Save to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click Apply to apply 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 large numbers of embedded, 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 is 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 Implementation Guide or Online Help (UHS).

# 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. Schedule LiveUpdate to occur at the same time for each protection engine if you use multiple protection engines to support virus scanning. 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 NAS device.

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 that 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.

### 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**, check **Enable scheduled LiveUpdate**. This option is enabled by default.
4. In the LiveUpdate interval list, choose 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:
   - Click **Save** to save your changes. You can continue to make changes in the administrative interface until you are ready to apply them.
   - Click **Apply** to apply 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 configure Symantec Protection Engine to retrieve Rapid Release definitions every 5 minutes to

every 120 minutes. Rapid Release definitions are created when a new threat is discovered. Rapid Release 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 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. Symantec encourages users to 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 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.

## Configuring 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, to specify the interval between which you want Symantec Protection Engine to download Rapid Release definitions, do any of the following steps:

   - Type the interval.
   - Click the up arrow or down arrow to select the interval.

   You can select any number between 5 minutes and 120 minutes. The default value is 30 minutes.
5. On the toolbar, select one of the following:

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

# Configuring the Hitachi NAS device

You must register at least one Symantec Protection Engine for each Hitachi NAS device for which you provide virus scanning. You also must configure the virus scan functionality in accordance with the Hitachi documentation.

For more information, please see the *Hitachi NAS Platform Antivirus Administration Guide* that is included in the HNAS Platform Product Documentation Library disc.

See "Configuring Symantec Protection Engine"

## About registering Symantec Protection Engine

You must register at least one Symantec Protection Engine to provide the virus scanning for each Hitachi NAS device. In a typical environment, a minimum of two protection engines are required to handle the scan volume per system. Having one protection engine can cause denial-of-file access, in which case the engine does not respond.

**Note:** You do not need to register the same protection engine with each Hitachi NAS device. You can register different protection engines to different Hitachi NAS devices. However, all the protection engines that are registered with the Hitachi NAS device must have identical configurations.

## About handling infected files on the NAS device

HNAS passes the clean files to the requesting user after it receives the scanning results. The stored version of the infected file is then replaced with the repaired file. The user is denied access to the file found to be infected and cannot be repaired. The infected file is subsequently deleted from HNAS. 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.

**Note:** In case of infected read-only files, SPE can scan the files, but cannot repair or delete them. However, the file's read only setting can be modified by using the HonorReadOnly command in order to repair or delete infected read only files.

If the file is infected, you are allowed access to the file, denied access to the file, or the file is deleted. You can configure these options on the NAS device. The infected file is deleted by default.

You can configure the NAS device to receive notifications when an infection is detected.

## About configuring virus scanning on the Hitachi NAS device

You must configure virus scanning for each Hitachi NAS device. The virusscan command is used to manage virus scanning settings. It can be used to manage virus scan servers, view statistics, set the file types that are scanned and to request a full system scan.

**Note:** The virus scan functionality for each Hitachi NAS device accessing a protection engine must be configured identically to avoid inconsistency. The scan results and repair results for infected files will be inconsistent if the settings differ for each device.

**virusscan [--on|--off] [-a] [-b <ip address>] [-d <ip address>] [-e <file types>] [-f] [-i <file types>] [-l] [-r] [-s] [-B | -N] [-I]**

**Options:**

-a, --all

Toggle functionality between scanning all files and scanning just those based on their extensions (see -I option for list of currently included file types).

-b, --enable <ip address|host>

Enable a virus scan server that isn't currently in use. Host names can only be used for ICAP scanners.

-d, --deregister <ip address|host>

Deregister a virus scan server that's currently registered. Host names can only be used for ICAP scanners. Note that in the case of RPC scanners, the virus scan server may simply re-register itself immediately. In this case, if you don't want the virus scan server to be used again, you should remove the current EVS's IP address(es) from the virus scan server's list of RPC clients.

-e, --delete <file types>

Delete the given file types from the list of file types to scan. Takes a comma-separated list.

-f, --default

Reset the list of file types to the default list.

-i, --include <file types>

Add the given file types to the list of file types to scan. Takes a comma-separated list. There can be a maximum of 250 entries in the list including the default types.

A wildcard '?' can be used to mean any single character. The matching is done per-character so the extension must match the length of the wildcarded extension. The wildcarded string "XL?" in the list will match .XLS and .XLX file extensions but will not match .XLSX extensions. To match .XLSX and .XLS files, for example, you would need to add both strings to the inclusion list (either with or without the wildcards - "XLS, XLSX", "XL?,XLS?" or ""XL?,XL??").

Multiple wildcards are acceptable - for example "A?C?" would match any four letter extension with "A" as its first character and "C" as its third (AACA, ..., ABCD, ..., AZCZ).

-l, --deleteall

Delete all file types from the list of file types to scan.

-r, --reset

Reset the statistics.

-s, --fullscan

Request a full system scan - i.e. scan all files in the list of file types to scan, regardless of whether they've been scanned already. Files won't be scanned immediately, but when they're next opened.

-I, --list-inclusion

Display a list of file types to scan, useful when virus-scanning is disabled (when the virus-scanning is enabled the list is displayed anyway).

-B, --enable-best-effort-scanning

Enable "best-effort" scanning. With this mode enabled CIFS access to files is not denied if there are no valid servers available. If no scan-engine is available, access will be granted to the user to open the file with no scan being performed. If a scan-engine reports a non-virus-related error during a scan, access will also be granted (see NOTE). The file is not marked in the file-system as "clean" so future accesses will prompt another attempted scan.

---

**Note:** Access is also enabled for files that cause a scan-engine to refuse to scan. For example, scan-engines usually have a maximum depth of zip file they will scan into before giving up. In best-effort mode these files will be available to be read. The intention of this is that access will be allowed unless a scan-engine specifically marks a file as infected.

---

-N, --disable-best-effort-scanning

Disable "best-effort" scanning. The normal operating mode where CIFS access is denied if the system cannot perform a scan due to lack of scan-engines.

-v, --verbose-stats

Show verbose server statistics. Each server keeps track of a number of extra statistics which can be used to diagnose virusscan scan-engine problems.

# About specifying file types on the NAS device

Based on file extensions, the NAS device determines, initially, whether it should pass a file to Symantec Protection Engine for scanning. You can configure which files are passed to Symantec Protection Engine for scanning when you set up the Hitachi NAS device.

You can control which files are scanned by using an exclusion or an inclusion list, or you can scan all files regardless of extension. Configure the Hitachi NAS device to pass all file types to the protection engine except those that are contained in the exclusion list. The exclusion list can include extensions for those file types that are not likely to contain viruses and can be excluded from scanning.

The virusscan command is used to configure the exclusion list.

**virusscan-exclusion-list-add <file-types>**

**Description**

The virusscan-exclusion-list-add command adds one or more file type extensions to the list of those which are to be excluded from virus scanning.

Options:

<file types>

A comma-separated list of file type extensions.

A wildcard '?' can be used to mean any single character. The matching is done per-character so the extension must match the length of the wildcarded extension. The wildcarded string "XL?" in the list will match ".XLS" and ".XLX" file extensions but will not match ".XLSX". To match ".XLSX" and ".XLS" files would require both to be added to the list (either with or without the wildcards - "XLS, XLSX", "XL?,XLS?" or "XL?,XL??").

Multiple wildcards are permitted within an extension. For example, "A?C?" will match any four letter extension with "A" as its first character and "C" as its third (AACA, ..., ABCD, ..., AZCZ).

There must be no whitespace between consecutive types.

**Examples**

To add the .bat, .com, .doc, .exe and .ppt types:

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

# Recommendations while integrating multiple protection engines

Do the following when multiple protection engines are used to support the Hitachi NAS device:

- 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. This ensures that virus definitions are consistent.
- Configure the virus scan functionality to be identical for each Hitachi NAS device in a group to avoid inconsistency. The scan results and repair results for infected files will be inconsistent if the settings differ for each device in the group.