Symantec™ Central Quarantine Implementation Guide

Symantec™ Central Quarantine Implementation Guide

Document Number: 11.00.00.00.00

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product feature and function, installation, and configuration. The Technical Support group also authors 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 maintenance 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
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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 recreate 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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 insurance and maintenance contracts
- Information about the Symantec Value License Program
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

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

- Asia-Pacific and Japan: contractsadmin@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com

Additional Enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

Introducing Symantec Central Quarantine

This chapter includes the following topics:

About Symantec Central Quarantine

When Symantec Endpoint Protection finds an infected item that cannot be repaired with the current virus definitions, it blocks access to the item. The products then package the item along with any affected system files and settings, and move the package to the local Quarantine. The local Quarantine is a special location that is reserved for infected files and related system side effects. After viruses and other threats are isolated in a local Quarantine, they are unable to damage or spread on the computer.

Symantec Endpoint Protection can automatically forward the packages that contain the infected files and their related side effects from a local Quarantine to the Central Quarantine. The Central Quarantine is a central repository. The Central Quarantine consists of two components: the Quarantine Server and the Microsoft Management Console (MMC) snap-in.

In addition to scanning files for viruses, Symantec Endpoint Protection clients scan files for security risks, which include spyware, adware, hacking tools, and joke programs. You can also forward these infected files to the Central Quarantine.

Threats that are detected and quarantined with Proactive Threat Protection, however, are submitted with a different mechanism.

Central Quarantine components

Table 1-1 describes the Symantec Central Quarantine components.

Table 1-1 Central Quarantine components

Component	Description
Symantec Security Response	The automated analysis center that reviews and analyzes submissions and creates and distributes updated virus definitions.
Gateway	The intermediary between Symantec Security Response and the Central Quarantine. Samples are analyzed and forwarded to Symantec Security Response only if they cannot be repaired with definitions on the gateway. If the sample can be repaired, definitions are returned from the gateway to the Central Quarantine.
Quarantine Console	The Central Quarantine user interface that is used to configure Quarantine Server operations, communicate with the gateway, and manage definitions updates.
Quarantine Server	The component that accepts infected files and side effects from servers and clients and communicates with the Quarantine Console. Items that arrive in the Quarantine are scanned with the Quarantine Server's set of definitions and submitted if they cannot be repaired. The Quarantine Server should be configured to listen on specific ports on IP protocols. A forwarding client must be configured to forward to the port that corresponds to the client's forwarding protocol.
Quarantine Agent	The component that handles communications between the Quarantine Server and the gateway, and triggers the Defcast mechanism. The Quarantine Agent ensures that the Central Quarantine has the latest set of definitions from the gateway.
Quarantine Scanner	The component that scans submitted files with the Quarantine Server's set of definitions. Samples that arrive in the Central Quarantine must be scanned before they can be submitted.

Table 1-1 Central Quarantine components *(continued)*

Component	Description
Defcast	The component that queries servers and clients for their virus definitions sequence number.
Alert Management System (AMS)	The Quarantine Server can be configured to take advantage of an AMS server, if installed. The Quarantine Server has its own set of AMS Events and Actions and its own AMS Log.

How Central Quarantine works

Central Quarantine uses the Digital Immune System to manage the entire antivirus process, from virus discovery on the desktop to virus analysis and side effect analysis. The Digital Immune System eliminates many of the manual tasks that are involved in the submission processes and analysis processes. Automation reduces the time between when a virus is first found and when a repair is deployed with LiveUpdate.

The Digital Immune System does the following:

- Identifies and quarantines: Rapidly identifies new threats by using powerful heuristic and behavioral detection. Suspicious items are isolated in the Central Quarantine and samples are automatically submitted to Symantec Security Response for analysis.
- Analyzes: Submits the files to Symantec Security Response for analysis, repair, and testing.

About identifying and quarantining viruses

The first goal of the Digital Immune System is to detect new or unknown threats at the desktop, server, and gateway. Symantec uses Bloodhound heuristics technology, which is designed to detect a majority of new or unknown viral strains.

You can configure clients to automatically send suspect files and their side effects to a local Quarantine. A local Quarantine may be located on the desktop, server, or gateway. The local Quarantine packages suspicious files with information about the submitting computer, then forwards the files to the corporate Central Quarantine for further analysis.

Since the Central Quarantine may have more up-to-date virus definitions than the submitting computer, it scans files by using its own set of virus definitions. If the Central Quarantine cannot fix a file, it strips the file of potentially sensitive

data if configured to do so, and then encrypts it. The Digital Immune System then transmits the file over the Internet to a Symantec gateway for further analysis.

Administrators can configure the Digital Immune System to automatically do the following:

- Detect and quarantine new and unknown viruses.
- Filter and forward encrypted samples to Symantec Security Response for analysis. The Digital Immune System can strip out sensitive content.
- Check for new virus definitions and status updates.

About analyzing viruses

The Quarantine Agent handles the communication between the Central Quarantine and the Symantec gateway. If the Central Quarantine cannot repair an infected file, the Quarantine Agent forwards it to the gateway. The Quarantine Agent then queries the gateway to see if the repair is ready

If the repair is ready, the Quarantine Agent downloads the new virus definitions set and installs the new definitions on the Central Quarantine. If the repair is not ready, the Quarantine Agent polls the gateway every 60 minutes for a repair.

When the Digital Immune System receives a new submission, it does the following:

- Adds the submission to a tracking database.
- Filters the submission to eliminate clean files, false positives, known viruses, and expanded threats. Filtering is quick, and because most submissions are resolved by filtering, the response time for filtered items is fast.
- Analyzes the virus and side effects, generates a repair, and then tests the repair. In most cases, analysis and repair are automatically generated, but some viruses may require the intervention of Symantec Security Response researchers.
- Builds a new virus definitions set, which includes the new fingerprint, and returns the new definitions to the gateway.

What you can do with Central Quarantine

Previous versions of the Central Quarantine pushed newly received virus and threat definitions to all the legacy clients that sent quarantined submissions to the Central Quarantine. This version of Central Quarantine still sends submissions to Symantec Security Response and receives updates for those submissions. However, this version does not push these definitions to clients that run Symantec Endpoint Protection.

Nevertheless, Central Quarantine provides a single source to co-locate all quarantined items on your network. All quarantined items appear in one window and they are automatically submitted to Symantec Security Response. This window also provides information about the submitted threats, such as the user and the computer that caught the threat. This window also shows the status of definitions that are created to detect the unknown threats that you submit.

The Digital Immune System feeds the information about the submitted threats to the Symantec Global Intelligence Network, which provides unparalleled insight into the Internet security landscape. Symantec Global Intelligence Network consists of more than 150 million desktop antivirus sensors, 40,000 intrusion detection and firewall sensors, and 4,300 monitored and managed security devices worldwide. This information is combined with Symantec's vulnerability database of 13,000 entries, which is the world's largest. These entries cover 30,000 versions of applications and operating systems from more than 4,000 vendors.

Where to get more information about Central Quarantine

You can find the primary documentation about Central Quarantine in the Docs folder on the installation CDs. Some individual component folders contain component-specific documentation. Updates to the documentation are available from the Symantec Technical Support and Platinum Support Web sites.

Table 1-2 lists the additional information that is available from the Symantec Web sites.

Table 1-2 Symantec technical support Web sites

Types of information	Web address
Public Knowledge Base Releases and updates Manuals and documentation Contact options	http://www.symantec.com/techsupp/enterprise/
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Platinum Support Web access	https://www-secure.symantec.com/platinum/

Chapter 2

Installing and configuring the Central Quarantine

This chapter includes the following topics:

Before you install

Before you install the Central Quarantine, you must consider the following:

- Administrator rights are required to install the Quarantine Console and the Quarantine Server. Make sure that you have proper rights before installing.
- Before installing Central Quarantine, make sure that you uninstall any previous version of Central Quarantine that exists on the computer.
- The Central Quarantine is composed of the Quarantine Server and the Quarantine Console. You can install the Quarantine Server and the Quarantine Console on the same computers or different computers with Windows 2000/XP/2003.
- The Quarantine Console must share a network protocol (TCP/IP) with the Quarantine Server to configure it.
- Quarantine-enabled products can forward files to the Quarantine Server using TCP/IP. Ensure that this network protocol is installed on the Quarantine Server.

System requirements for the Central Quarantine Server

Installing the Central Quarantine Server requires the following system requirements:

- Windows 2000 Professional/Server/Advanced Server, XP Professional, Server 2003 Web/Standard/Enterprise/Datacenter
- Microsoft Internet Explorer 5.5, Service Pack 2, 128-bit encryption, or later
  If you install Symantec Endpoint Protection on this computer, Microsoft Internet Explorer 6.0 or later is required.
- 128 megabytes (MB) of RAM
- Minimum swap file size of 250 MB
- 40 MB of available disk space
- 500 MB to 4 GB of available disk space for quarantined items

Note: If you run Windows XP, system disk space usage is increased if the System Restore functionality is enabled. For more information on how System Restore functionality is enabled, see the Microsoft operating system documentation.

System requirements for the Quarantine Console

Installing the Quarantine Console requires the following system requirements:

- Windows 2000 Professional/Server/Advanced Server, XP Professional, Server 2003 Web/Standard/Enterprise/Datacenter
- Microsoft Internet Explorer 5.5, Service Pack 2, 128-bit encryption, or later
  If you install Symantec Endpoint Protection on this computer, Microsoft Internet Explorer 6.0 or later is required.
- 64 MB RAM
- 35 MB of disk space
- Microsoft Management Console 1.2

Note: If Microsoft Management Console is not installed, you need 3 MB of free disk space (10 MB during installation).

Installing the Central Quarantine

Installing the Central Quarantine consists of the following tasks in the following order:

- Installing the Quarantine Console
- Installing the Quarantine Server

Note: Install the Quarantine Console first and then install the Quarantine Server. If you do not follow this order, the AMS is not properly configured. If you do not follow this order and want to properly configure AMS, associate AMS with the Quarantine Server with the Alerting Properties. Then restart the Quarantine Server.

To install the Quarantine Console

1. Start the installation, and then click **Install Other Administrator Tools**.
2. Click **Install Central Quarantine Console**.
3. In the Welcome dialog box, click **Next**.
4. In the License Agreement dialog box, select **I accept the terms in the license agreement**.
5. Click **Next**.
6. In the Destination Folder dialog box, select one of the following:
   - Next: To install to the default folder.
   - Change: To select a different folder.
     Do not install the Quarantine Console on a network drive.
7. Follow the on-screen directions to complete the installation.

To install the Quarantine Server

1. Start the installation, and then click **Install Other Administrator Tools**.
2. Click **Install Central Quarantine Server**.
3. In the Welcome dialog box, click **Next**.
4. In the License Agreement dialog box, select **I accept the terms in the license agreement**.
5. Click **Next**.
6. In the Destination Folder dialog box, select one of the following:
   - Next: To install to the default folder.

- Change: To select a different folder.
  The Quarantine Server should not be installed on a network drive.

7. In the Setup Type dialog box, click **Internet based (Recommended).**
8. Click **Next**.
9. In the Maximum Disk Space dialog box, either accept the default disk space of 500 megabytes, or type a new value (in megabytes) in the Disk space box, then click **Next**.
10. In the Contact Information dialog box, type your company's name, account number (if available), contact name, contact telephone, and contact email.
11. Click **Next**.
12. In the Web Communication dialog box, either accept the default gateway address, or type another address (if provided by Symantec) in the Gateway Name box. Then click **Next**.
13. In the Alerts Configuration dialog box, click **Enable Alerts** if you use Alert Management Server (AMS). Type the name of your AMS server and then click **Next**.
14. Follow the on-screen directions to complete the installation.

Chapter 3

Using the Central Quarantine

This chapter includes the following topics:

Enabling and configuring the Central Quarantine

The Central Quarantine is composed of two primary components, the Quarantine Server and the Quarantine Console. The Quarantine Server stores infected samples and communicates with Symantec Security Response. The Quarantine Console, which snaps into Microsoft Management Console, lets you manage the Quarantine Server.

To use the Central Quarantine, do the following:

- Enable the Quarantine Server.
- Configure the Quarantine Server.
- Configure the clients to forward samples to the Quarantine Server.

Enabling the Quarantine Server

You can enable the Quarantine Server on the local computer and on a remote computer.

To enable the Quarantine Server on the local computer

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, and then click **Attach to server**.
2. In the Select Computer dialog box, click **This computer**, and then click **OK**.

To enable the Quarantine Server on a remote computer

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, and then click **Attach to server**.
2. In the Attach to Quarantine Server dialog box, type the server name.
3. Type the user name and password to log on to the server.
4. If the server is part of a domain, type the domain name as well.

Configuring the Quarantine Server

You configure the Quarantine Server with the following information:

- The folder location to store files on the Quarantine Server
- The protocol and port on which to listen

After the Quarantine Server is configured, you configure clients to send copies of the files that are contained in their local Quarantines.

Note: The Quarantine Console user interface lets you select the IP or SPX protocol and specify the port number to configure. This IP protocol and port number is TCP and is the listening port. Do not select SPX. Also, the TCP port number that you enter is not what appears when the ports are displayed with tools like netstat -a. For example, if you enter port number 33, netstat -a displays TCP port 8448. The hexadecimal and decimal numbers transpose and improperly convert. For details, see http://entsupport.symantec.com/docs/n2000081412370148.

To configure the Quarantine Server

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, and then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the General tab, type the folder location for the Central Quarantine.
3. Under Maximum Allowable Size, specify the maximum size for the Quarantine.

4 Under Protocols, check **Listen on IP** (TCP/IP).

Do not check Listen on SPX.

5 In the Port box, type the port number on which to listen, and then click **Apply > OK**.

The default port number is 33.

Configuring an antivirus policy to use the Quarantine Server

Symantec Endpoint Protection clients in a group or a group's location must use an antivirus policy that forwards the quarantine samples to the Quarantine server. The policy requires you to enter the fully-qualified domain name (recommended) or IP address of the Quarantine server. The policy also requires you to enter the protocol and port number that you specified for the Quarantine server's listening port.

To configure an antivirus policy to use the Quarantine Server

1 In the Symantec Endpoint Protection Manager Console, click **Policies**.

2 In the View Policies pane, click **AntiVirus**.

3 In the lower-left What would you like to do pane, click **Add an AntiVirus Policy**.

You can also edit an existing policy.

4 In the AntiVirus Policy window, in the left pane, click **Submissions**.

5 Under Quarantined Items, check **Allow client computers to automatically submit quarantined items to a Quarantine Server**.

6 In the Server name box, type the fully-qualified domain name or IP address of the Quarantine Server.

7 In the Port number box, accept or change the default port number.

8 In the Retry box, accept or change the retry interval when client to Quarantine Server communications fail.

9 In the Protocol drop-down list, verify that IP is selected only.

10 Click **OK**.

11 Apply the policy to one or more groups.

Central Quarantine properties

Table 3-1 provides a brief description of the configuration property settings that are available and supported for the Central Quarantine.

Note: Central Quarantine's default settings use the information that is provided during the installation to offer comprehensive protection without further configuration. You do not need to change any of these settings.

Table 3-1 Central Quarantine properties

Property	Description
General	This property lets you specify the primary quarantine settings, such as the folder location of the Quarantine. And settings for the maximum size of the folder's contents, the listening protocol for communication with clients, and the console auto-refresh interval.
Web Communication	This property lets you specify communication settings, including the computer name of the Symantec gateway and the following security settings: ■ Secure submission sends virus samples to Symantec by using secure sockets Layer (SSL). ■ Secure download uses SSL to receive updated definitions from Symantec. ■ Symantec Immune System Gateway specifies the gateway computer that communicates with Symantec Security Response.
Firewall	This property lets you specify how to communicate with and through a proxy firewall, if your network uses a proxy firewall: ■ Firewall name is the IP address or the name of the firewall. ■ Firewall port is the port on which to communicate with the firewall. ■ Firewall user name is the user name to communicate with the firewall. ■ Firewall password is the password to communicate with the firewall.

Table 3-1 Central Quarantine properties *(continued)*

Property	Description
Sample Policy	This property lets you specify how samples are submitted and processed: ■ Automatic sample submission automatically queues virus samples for analysis. ■ Queue check interval is the frequency at which the Quarantine is checked for new items. ■ Strip user data from sample maintains security by removing potentially sensitive data from sample submissions. ■ Status query interval is the frequency at which the gateway is polled for status changes about submitted samples.
Definition Policy	This property lets you specify how antivirus and antispyware definitions are processed: ■ Active sequence number is the sequence number of the currently installed definitions on the Quarantine Server. Sequence numbers are used only by Symantec AntiVirus products, are assigned to signature sets sequentially, and are always cumulative. A signature set with a higher sequence number supersedes a signature set with a lower sequence number. ■ Certified definitions interval is the frequency, in minutes, for polling the gateway for updated certified definitions. The default setting is three times a day.
Customer Information	This property lets you edit the customer information that you entered during the installation. All fields are required.
Alerting	This property lets you configure the alerting for specific events. If you add the AMS server here, you must restart the Quarantine Server before you can configure events.
General Errors	This property lists the history of the Quarantine Server errors.

Managing quarantined files

By default, Symantec Endpoint Protection clients isolate the infected items that cannot be repaired with their current sets of virus definitions. Clients that have

been configured to forward these infected files and their side effects automatically send copies to the Central Quarantine Server.

Viewing the quarantined items

Files are added to the Central Quarantine when client computers are configured to forward the infected items to the Quarantine Server.

Table 3-2 shows the information that is reported.

Table 3-2 Quarantined file information

Property	Description
File name	Name of the infected item
User name	User whose file was infected
Computer	Computer on which the infected item was discovered
Analyzed	Indicates whether the sample was analyzed
Age	Date that the sample was quarantined
Sample state See "Sample State" on page 34.	Current state of the sample
Definitions Needed	Sequence number of the definitions set that is needed to resolve the virus
Status See "Sample Status" on page 33.	Processing state of the sample
Virus	Name of the virus that is identified
Errors See "Sample errors" on page 38.	Sample processing errors

To view the quarantined items

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.

   Quarantined items are listed in the right pane.

2. In the right pane, right-click a quarantined item, and then click **Properties**.

Deleting the quarantined files

Although you can delete any item that is in the Central Quarantine, reserve this option for the files that you no longer need. After you confirm that the updated definitions have detected and eliminated the virus, it is safe to delete the quarantined item.

To delete the quarantined files

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click one or more files, and then click **Delete**.

Restoring quarantined files

When you choose to restore a file, no attempt is made to repair it. Use this option with discretion to avoid the risk of infecting your system. For example, you should restore a file only when Symantec Security Response notifies you that a submitted file is not infected. Restoring a potentially infected file is not safe. Restored files are copied to a folder location that you specify.

To restore quarantined files

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click one or more files, and then click **All Tasks > Restore Item**.
3. If you are sure that you want to restore the file, click **Yes**.
4. In the Browse for Folder dialog box, select a location to restore the file, and then click **OK**.

Submitting samples for analysis

Sample Policy settings determine whether or not the virus samples are submitted automatically to the gateway. If automatic sample submission is not selected, each sample in the Quarantine must be manually released to the gateway.

The Policy settings for automatic sample submission can be overridden. Generally, the samples are submitted manually only when a submission error or a change to the queue priority of selected samples is desired.

Setting an automatic sample submission policy

Sample Policy settings determine whether or not the virus samples are submitted automatically to the gateway. If automatic sample submission is not selected, the samples in the Quarantine must be released to the gateway individually.

For additional security, you can specify that user data be stripped from the sample before submission.

Note: You can supersede the Policy submission settings on an item-by-item basis when you view the Actions tab for a selected item in the Quarantine.

To set an automatic sample submission policy

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, and then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the Sample Policy tab, set the sample policy.

Submitting files manually

Suspect files can be manually submitted for virus analysis. Samples that can be repaired with the definitions that reside on the Quarantine Server or the gateway are not sent to Symantec Security Response.

To be eligible for manual submission, a sample must meet the following conditions:

- The sample cannot already be eligible for automatic submission (X-Sample-Priority must be 0).
- The sample has not already been submitted (X-Date-Submitted is missing or 0).
- The sample has not already been analyzed (X-Date-Finished is not present or 0).

You must set the priority for a sample before you can submit files manually.

To set the priority for a sample manually

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click an item, and then click **Properties**.
3. In the Symantec Central Quarantine Properties dialog box, on the Actions tab, set the submission priority.

To submit items manually to Symantec Security Response

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click one or more files, and then click **All Tasks > Queue item for automatic analysis**.

Reviewing sample submission status

You can determine a sample's status by reviewing the actions and the attributes that were set during the communications between the Quarantine Server and the gateway.

Viewing attributes for a sample

The request and the response messages that clients and servers exchange contain numerous attributes that describe a sample's completely and status. These proprietary attributes always start with the X- characters.

To view attributes for a sample

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**.
2. In the right pane, right-click an item, and then click **Properties**.
3. In the Properties dialog box, on the Sample Attributes tab, double-click a displayed attribute for a brief definition of the attribute.

Reviewing the actions that were taken on a sample

The actions that were taken on a sample include a selected sample's submission and virus definitions delivery status.

You can override the default sample submission policy settings for the selected sample. You can manually queue a sample for submission to Symantec Security Response, as well as query for updated virus definitions files for the selected sample.

To review actions on samples

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click an item, and then click **Properties**.
3. In the Properties dialog box, on the Actions tab, review the actions that were taken on the sample.

Reviewing the submission errors for a sample

Submission errors, if any, are reported for each sample. Review the entries to determine what action is required for the sample.

To review the submission errors for a sample

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**.
2. In the right pane, right-click an item, and then click **Properties**.
3. In the Properties dialog box, on the Errors tab, review the submission errors.

Configuring events and alerts

You can specify the events that you want to know about. Your options are to send the event information to the NT event log, to AMS, or to both. If you send the event information to AMS, you must configure the type of alert that you want AMS to send.

Specifying the events that trigger alerts

Table 3-3 describes the events that can be monitored by sending notifications to the NT event log and AMS.

Table 3-3 Events that trigger alerts

Event	Description
Unable to connect to the Gateway	The Quarantine Agent cannot connect to the Digital Immune System gateway.
Defcast error	Defcast is the service that distributes new definitions from the Quarantine Server to target computers.
Cannot install definitions on target computers	The distribution of new definitions failed. Also indicates that definitions are available for nonmanaged clients.
Unable to access definition directory	The Quarantine Server cannot find the definitions directory.
Cannot connect to Quarantine Scanner svc	Samples cannot be scanned in the Quarantine and are not forwarded to the gateway.

Table 3-3 Events that trigger alerts *(continued)*

Event	Description
The Quarantine Agent service has stopped	The Quarantine cannot communicate with the gateway.
Waiting for needed definitions	Definitions have not yet arrived from the gateway.
New certified definitions arrived	New certified definitions have arrived on the Quarantine Server.
New non-certified definitions arrived	New non-certified definitions have arrived on the Quarantine Server in response to a sample submission.
Disk quota remaining is low for Quarantine dir	The Quarantine folder is nearly full.
Disk free space is less than Quarantine max size	The Quarantine folder is set to a maximum size that is greater than the available free disk space.
Sample: was not repaired	Either a sample was not repaired or a repair was not necessary.
Sample: unable to install definitions	New definitions could not be installed, usually due to a corrupted definitions set.
Sample: processing error	An error occurred while this sample was processed.
Sample: needs attention from Tech Support	The sample could not be processed automatically. Contact Tech Support for help with the sample.
Sample: held for manual submission	The sample is held on the Quarantine Server instead of being automatically submitted.
Sample: too long without installing new defs	New definitions should have been installed (status is distribute), but were not.
Sample: too long with Distributed Status	New definitions have arrived from the gateway, but confirmation that they were installed on the client has not yet been received at the Quarantine.
Sample: too long with Needed status	Definitions have not yet been pulled from the gateway.
Sample: too long with Released status	The gateway has not yet responded.

Table 3-3 Events that trigger alerts *(continued)*

Event	Description
Sample: too long with Submitted status	The gateway has not yet accepted the sample.
Sample: too long with Quarantined status	The sample has not yet been scanned initially at the Quarantine.
Sample: new definitions held for delivery	New definitions are held on the Quarantine Server instead of being delivered.

To specify the events that trigger alerts

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, and then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the Alerting tab, do one or both of the following:
   - To send events to AMS, check **Send Events to AMS**.
   - To send events to the NT event log, check **NT event log**.
3. Under Configure Event Notification, do one or both of the following:
   - Check the events that you want know about.
   - Uncheck the events that you do not want to know about.
4. Click **OK**.

Configuring the AMS alerts and responses

With AMS, you can configure the AMS alerts and responses.

To configure the AMS alerts and responses

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, and then click **Configure Quarantine Events**.
2. In the Central Quarantine Events, expand Central Quarantine.
3. Under Central Quarantine, click and highlight the event to configure, and then click **Configure**.
4. In the Select Action dialog box, click one of the following options, and then click **Next**:
   - Broadcast
   - Email
   - Message Box

- Load NLM
- NT Event Log entry
- Send Page
- Run Program
- Send SNMP Trap

5 In the Select Action dialog box, select the AMS server to generate the alert or response, and then click **Next**.

6 Follow the prompts to complete the configuration.

Appendix A

Sample processing reference

This appendix includes the following topics:

About sample processing

The Digital Immune System provides realtime information about any sample within the system, including the processing status and the analysis state of a submitted sample.

Sample Status

Table A-1 describes the Sample Status, which is the processing status of the sample within the Digital Immune System.

Table A-1 Sample Status

Status	Description
Attention	The sample requires intervention from technical support.
Available	New definitions are held for delivery to the submitting computer.

Table A-1 Sample Status *(continued)*

Status	Description
Distribute	New definitions are queued for delivery to the submitting computer.
Distributed	New definitions have been delivered to the submitting computer.
Error	A processing error occurred.
Held	The sample is withheld from submission.
Installed	New definitions have been installed on the submitting computer.
Needed	New definitions are required for the sample.
Not installed	Definitions cannot be delivered to the submitting computer.
Quarantined	The Central Quarantine received the sample.
Released	The sample has been queued for analysis.
Restart	Sample processing starts again.
Submitted	The sample has been submitted to Symantec Security Response for analysis.
Unneeded	New definitions are not required for the sample.

Sample State

Sample State is the analysis state of the submitted sample within the Digital Immune System. The state indicates where in the network hierarchy a sample is located, what stage of the analysis pipeline is currently working on the sample, or its final disposition.

Note: Any state that infers that a sample was returned back to a client computer is no longer supported.

Final states

Samples that have been finished are in one of the final states. All nodes in the Digital Immune System use the terminal states. After a sample has been placed in a terminal state, its state does not change again. The X-Date-Analyzed attribute is set when a sample is placed into a terminal state; its presence means that the value of X-Analysis-State is terminal.

Table A-2 describes the final states.

Table A-2 Final states

State	Description
abort	An internal programming error has derailed transport or analysis of the sample.
attention	The sample requires intervention from technical support.
broken	The sample is infected with a virus, but the definition generation service in the back office reported an error. No virus definitions files are available.
declined	The sample is not acceptable, and has been refused.
error	A processing error occurred.
infected	The sample is infected with a virus, and can be repaired with available virus definitions files.
misfired	The sample has been analyzed and no virus was found, in spite of a detected infection. A mistake in previous virus definitions files caused the incorrectly detected infection and the mistake is corrected in newer virus definitions files.
nodetect	The sample has not been analyzed, but does not contain any apparent suspicious code.
norepair	The sample is infected with a virus, but it cannot be repaired with available virus definitions files. It should be deleted.
uninfectable	The sample contains no executable code, and therefore cannot be infected with any virus. The sample may be too small to contain any executable code, or may contain data only, such as a graphic image or an audio clip.
uninfected	The sample has been analyzed and no virus was found.
unsubmittable	The sample contains known malicious software, such as a worm or Trojan horse. It should be deleted.
encrypted	Central Quarantine cannot scan this sample because it is encrypted or password-protected. You need to decrypt it or remove the password protection before resubmitting it.
delete	Files either created by malicious code or that contain malicious code. The only action you can take on these files is to delete them.

Table A-2 Final states *(continued)*

State	Description
restore	Files that cannot be cleaned. The files may be altered accidentally or by a virus, and they may contain corrupted viral code. Due to the alterations, it is impossible or unsafe to retain the files. You should restore the files from a backup.

Transit states

Samples that have not yet reached Symantec Security Response are in one of the transit states. Only the components outside Symantec Security Response use the transit states. A sample may remain in a pending state indefinitely before it moves to another state.

Table A-3 describes the transit states.

Table A-3 Transit states

State	Description
accepted	A gateway accepted the sample, but the sample is not yet imported into Symantec Security Response.
importing	Symantec Security Response imported the sample.
receiving	A gateway received the sample.

Pending states

Samples that wait for analysis within Symantec Security Response are in one of the pending states. Only the components within Symantec Security Response use the pending states. A sample may remain in a pending state indefinitely before it moves to another state.

Table A-4 describes the pending states.

Table A-4 Pending states

State	Description
defer	The sample cannot be analyzed automatically, and is deferred for analysis by experts.
deferred	The sample cannot be analyzed automatically, and is deferred for analysis by experts.

Table A-4 Pending states *(continued)*

State	Description
deferring	The sample cannot be analyzed automatically, and is deferred for analysis by experts.
imported	The sample has been imported into Symantec Security Response, but has not yet been analyzed.
rescan	The sample must be rescanned because newer virus definitions files have become available within Symantec Security Response.

Active states

Samples that are being analyzed within Symantec Security Response are in one of the active states. Only the dataflow component within Symantec Security Response uses the active states. A sample may remain in an active state for only a few seconds or for many minutes before it moves to another state.

Table A-5 describes the active states.

Table A-5 Active states

State	Description
archive	The sample is waiting to archive the automated analysis files.
archiving	The sample is archiving the automated analysis files.
binary	The sample has been classified as a binary program, and is waiting for the binary controller.
binaryControlling	The binary controller is determining starting conditions for the binary replication.
binaryReplicating	The sample is being executed by a binary replication engine.
binaryScoring	The sample infected other binary programs, and the binary scoring engine is selecting signatures for detecting and repairing the virus.
binaryWait	The sample is waiting for a binary replication engine to become available.
classifying	The sample is being classified to determine its data type.
fullBuilding	A new set of virus definitions files incorporating the signatures that are selected for the new virus are being built.

Table A-5 Active states *(continued)*

State	Description
fullUnitTesting	The full virus definitions files are being unit-tested.
incrBuilding	The signatures that are selected for the new virus are being added to the current virus definitions files.
incrUnitTesting	The incremental virus definitions files are being unit-tested.
locking	Exclusive access to the definition generation service in the back office is being acquired.
macro	The sample has been classified as a document or a spreadsheet that contains executable macros, and is waiting for the macro controller.
macroControlling	The macro controller is determining starting conditions for macro replication.
macroReplicating	The sample is being executed by a macro replication engine.
macroScoring	The sample infected other documents or spreadsheets, and the macro scoring engine is selecting signatures for detecting and repairing the virus.
macroWait	The sample is waiting for a macro replication engine to become available.
signatures	The sample is infected with a new virus, signatures for detecting and repairing it have been selected, and the sample is waiting for the build process to become available.
unlocking	Exclusive access to the definition generation service is being released.

Sample errors

Sample processing errors include those listed in the following table.

Table A-6 describes the sample errors.

Table A-6 Sample errors

Error	Description
abandoned	A signature sequence number has been abandoned, usually because unit-testing of the corresponding definitions set has failed.
content	The sample's content checksum does not match its content.
crumbled	The sample's tracking cookie has not been assigned by the gateway.
declined	The sample that was submitted for analysis has been declined by the gateway. The user should contact technical support for assistance.
internal	An internal failure occurred while processing a sample.
lost	The sample was not completely received due to a network failure.
malformed	An essential attribute of the sample was malformed.
missing	An essential attribute of the sample was missing.
overrun	The content of this sample exceeds its expected length. This overrun may be due to a transmission error in the transport network.
sample	The sample's sample checksum does not match its content.
superseded	This signature sequence number has been superseded by newer certified definitions and is no longer available from the server. The client should download the current certified definitions instead of the superseded definitions.
type	The sample's type is not supported.
unavailable	The signature sequence number has not yet been published.
underrun	The expected length of the sample exceeds its content.
unpackage	The sample or signature cannot be unpacked.
unpublished	The signature set cannot be published.

Index

Q

S

V

W

X