Symantec™ Central Quarantine Administrator's Guide

Symantec™ Central Quarantine Administrator's Guide

Documentation version 8.0

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

Chapter 1

Introducing Quarantine

This chapter includes the following topics:

About Quarantine

When Symantec and Symantec AntiVirus products scan an infected item that cannot be repaired with their current set of virus definitions, they block access to the item and move it to a local Quarantine, a special location reserved for files that are infected by viruses. Once isolated in a local Quarantine, viruses are unable to spread into other areas of the infected computer.

Depending on their configuration, Symantec and Symantec AntiVirus products can automatically forward infected files from a local Quarantine to the Central Quarantine, a central repository for infected files. The Central Quarantine consists of two components: the Quarantine Server and the Quarantine Console, a Microsoft Management Console (MMC) snap-in. The Central Quarantine may be configured to scan and deliver infected files in two ways:

- Internet-based Scan and Deliver: A fully automated system for submitting infected files to Symantec Security Response (formerly known as Symantec AntiVirus Research Center, or SARC) for analysis and repair
- Email-based Scan and Deliver: A semi-automated system that requires administrator intervention to handle infected file submissions and virus definitions delivery

Both forms of Scan and Deliver take advantage of Symantec's Digital Immune System.

About the Digital Immune System

Earlier generation antivirus software aimed to protect the desktop from viral threats. In the late 1990s, the damage caused by infamous viruses such as Melissa demonstrated that protecting the desktop is not enough. Although many of the desktops and servers affected by Melissa were protected by up-to-date antivirus software, they were unable to fend off the virus.

Symantec developed the Digital Immune System to address the limitations of existing antivirus software. The Digital Immune System is a fully automated, closed-loop antivirus system. The Digital Immune System manages the entire antivirus process, from virus discovery on the desktop, virus analysis at the antivirus provider, and deployment of a repair to the affected desktop. In addition, the Digital Immune System eliminates many of the manual tasks involved in the submission, analysis, and distribution processes. Automation dramatically reduces the time between when a virus is first found and when a repair is deployed, decreasing the severity and virulence of many virus threats.

The Digital Immune System does the following:

- Identifies and quarantines: Rapidly identifies new viruses 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 files to Symantec Security Response for analysis, repair, and testing.
- Repairs: Automatically delivers the repair to customer sites.

Identifying and quarantining viruses

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

If configured to do so, clients automatically send suspect files to a local Quarantine, which may be located on the desktop, server, or gateway. From the local Quarantine, suspicious files are then packaged with information about the submitting computer, and forwarded from the local Quarantine 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 using its own set of virus definitions. If the Central Quarantine can fix a file, it pushes the newer virus definitions set to the affected computer. If the Central Quarantine cannot fix a file, it strips the file of potentially sensitive data (for example, text is removed from Word files), and 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 run automatically to do the following:

- Detect and quarantine new and unknown viruses.
- Filter and forward encrypted samples to Symantec Security Response for analysis (stripping sensitive content, if desired).
- Check for new virus definitions and status updates.
- Deploy new definitions to the infected computer or to a larger set of computers.

See "Digital Immune System and Central Quarantine components" on page 9.

See "Enabling and configuring Internet-based Central Quarantine" on page 28.

Analyzing viruses

The Quarantine Agent handles communication between the Central Quarantine and the Symantec gateway. If the Central Quarantine cannot fix an infected file, the Quarantine Agent forwards it to the gateway. The Quarantine Agent then queries the gateway to see if the issue has already been resolved.

- If the issue has been resolved, the Quarantine Agent downloads the new virus definitions set and installs the new definitions on the Central Quarantine. Next, the Quarantine Agent checks whether or not the submitting computer needs the updated definitions set, and pushes the new definitions to the affected computer, if required.
- If the issue has not yet been resolved, the Quarantine Agent begins to poll 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, eliminating clean files, false positives, and known viruses. Filtering is quick, and since most submissions are resolved via filtering, the response time for filtered items is very fast.
- Analyzes the virus, 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, including the new fingerprint, and returns the new definitions to the gateway.

Repairing the infection

When the Quarantine Agent polls the gateway and receives notification that a repair is available, it downloads the virus definitions set and installs it on the Central Quarantine. Next, the Quarantine Agent checks whether or not the submitting computer needs the updated definitions set, and pushes the new definitions to the affected computer, if required.

Digital Immune System and Central Quarantine components

The Digital Immune System and the Symantec Central Quarantine are composed of the components listed in Table 1-1.

Table 1-1 Digital Immune System and Central Quarantine components

Component	Description
Symantec Security Response	Automated analysis center that reviews and analyzes submissions and creates and distributes updated virus definitions.
Gateway	Intermediary between Symantec Security Response and the Central Quarantine. Samples are analyzed and only forwarded to Symantec Security Response 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	Central Quarantine user interface used to configure Quarantine Server operations, communicate with the gateway, and manage definitions updates.
Quarantine Server	Component that accepts infected files 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 is configured to listen on specific ports on both IP and SPX protocols. A forwarding client must be configured to forward to the port corresponding to the client's forwarding protocol.
Quarantine Agent	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.

Table 1-1 Digital Immune System and Central Quarantine components

Component	Description
Quarantine Scanner	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. The definitions that are downloaded by the agent and used by the Quarantine Scanner are separate from all other virus definitions sets used by other Symantec AntiVirus products on the Quarantine Server computer.
Defcast	Component that queries servers and clients for their virus definitions sequence number and pushes out new definitions sets, as necessary.
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.

See "Configuring alerting" on page 46.

See "About the Digital Immune System" on page 6.

See "Enabling and configuring Internet-based Central Quarantine" on page 28.

About Internet-based Scan and Deliver

In an Internet-based Scan and Deliver configuration, the Central Quarantine Server (if configured to do so) automatically submits samples of the infected items to Symantec Security Response for analysis and repair without administrator intervention. When Symantec Security Response receives an infected item from an Internet-based submission, it analyzes the submission and then delivers updated virus definitions to the affected customer over the Internet. The new definitions are automatically installed on the Quarantine Server, and, depending on the configuration, the gateway, server, or desktop that originally submitted the infected file.

About email-based Scan and Deliver

In an email-based configuration, administrators manually email suspicious files to Symantec Security Response for analysis and repair. The Quarantine Console provides a Scan and Deliver Wizard that makes this an easy task. Symantec Security Response analyzes the submission, and then emails the repair back to an administrator at the infected site in the form of new virus definitions files.

See "Using email-based Scan and Deliver" on page 17.

Deciding which form of Scan and Deliver to use

You make the decision on whether to use email-based or Internet-based Scan and Deliver during installation.

- Use email-based Scan and Deliver if you want to manually submit virus samples to Symantec Security Response, and manually apply new virus definitions to the computers in your network.
- Use Internet-based Scan and Deliver if you want the Quarantine Server to automatically submit virus samples to Symantec Security Response, and automatically apply new virus definitions to the computers in your network.

About Symantec Security Response

At Symantec Security Response, a dedicated team of virus experts works around the clock to develop technology to find and eliminate computer viruses. Researchers are aided by Symantec AntiVirus Research Automation (SARA). SARA automatically analyzes a high percentage of virus sample submissions. These automated virus definitions are created and distributed to customers rapidly and without human intervention, stopping newly discovered viruses before they can spread.

Chapter 2

Installing and configuring the Central Quarantine

This chapter includes the following topics:

Before you install

Before installing 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.
- The Central Quarantine is composed of the Quarantine Server and the Quarantine Console. The Quarantine Server and the Quarantine Console can be installed on the same or different Windows NT/2000 computers.
- The Quarantine Console must share a network protocol (either TCP/IP or IPX/SPX) with the Quarantine Server in order to configure it.
- Quarantine-enabled products can forward files to the Quarantine Server using TCP/IP or IPX/SPX, so ensure that both of these network protocols are installed on the Quarantine Server.
- If you plan on using Internet-based Scan and Deliver, ensure that the Quarantine Server has an Internet connection to take advantage of automated virus submission and virus definitions updating. In addition, ensure that your firewall or HTTP proxy server allows the Quarantine Server to access the Internet.

System requirements for the Central Quarantine Server and Console

- Windows 2000/NT Server 4.0 with Service Pack 5 or later
- Windows NT Server DCOM module (for Windows NT Server 4.0 only)
- Internet Explorer version 5.5, Service Pack 2, 128-bit encryption, or later
- 128 MB RAM
- Minimum paging file size of 250 MB
- 15 MB available disk space
- Up to 4 GB available disk space for quarantined items
- Local administrator rights to Windows NT servers or Windows NT domain

Installing the Central Quarantine

Installing the Central Quarantine consists of the following tasks:

- Installing the Quarantine Console
- Installing the Quarantine Server

Note: If your Symantec product provides an autoinstall for the Quarantine Console and the Quarantine Server, disregard the following procedure.

To install the Central Quarantine

To install the Central Quarantine, you must install the Quarantine Console and the Quarantine Server.

To install the Quarantine Console

1. In the Symantec Client Security Installation dialog box, click **Install SAV Administrator Tools**.
2. Click **Install Central Quarantine Console**.
3. In the Welcome window, click **Next.**
4. In the License Agreement window, click **Yes.**
5. In the Choose Destination Location window, select one of the following:
   - Next: To install to the default folder.
   - Browse: To select a different folder.
     Do not install the Quarantine Console on a network drive.
6. Follow the on-screen directions to complete the installation.

To install the Quarantine Server

1. In the Symantec Client Security Installation dialog box, click **Install SAV Administrator Tools**.
2. Click **Install Central Quarantine Server**.
3. In the Welcome window, click **Next.**
4. In the Choose Destination Location window, select one of the following:
   - Next: To install to the default folder.
   - Browse: To select a different folder.
     The Quarantine Server should not be installed on a network drive.

5 In the Setup Type window, select one of the following:

- Internet based (Recommended)

  See "Using Internet-based Scan and Deliver" on page 27.

- Email based

  See "Using email-based Scan and Deliver" on page 17.

6 Click **Next**.

7 In the Maximum Disk Space window, either accept the default disk space of 500 megabytes, or type a new value in the Disk space (megabytes) box, then click **Next**.

8 In the Customer Information window, type your company's name, account number (if available), contact name, contact telephone, and contact email. All fields are required, then click **Next**.

9 In the Web Communication window, either accept the default gateway address, or type another address (if provided by Symantec), then click **Next**.

10 In the Alerts Configuration window, click **Enable Alerts** if you are using Alert Management Server (AMS), type the name of your AMS server, then click **Next**.

11 Follow the on-screen directions to complete the installation.

Configuring the Central Quarantine

The Central Quarantine's default settings use the information provided during installation to provide comprehensive protection without further configuration.

See "Central Quarantine Properties" on page 31.

See "Configuring email-based client forwarding" on page 20.

See "Configuring Internet-based client forwarding" on page 33.

See "Configuring alerting" on page 46.

Chapter 3

Using email-based Scan and Deliver

This chapter includes the following topics:

About email-based Scan and Deliver

Email-based Scan and Deliver uses email to:

- Submit samples to Symantec Security Response using the Scan and Deliver Wizard.
- Receive new virus definitions when a new virus is found.

Enabling and configuring email-based Central Quarantine

The Central Quarantine is composed of two components: the Quarantine Server, which is installed on any Windows NT/2000 computer to store infected samples and communicate with Symantec Security Response, and the Quarantine Console that snaps into MMC to perform management tasks.

To use the Central Quarantine, do the following:

- Enable the Quarantine Server.
- Configure the Quarantine Server.
- Configure clients to forward to the Quarantine Server.
- Configure Scan and Deliver to transport samples to Symantec Security Response and receive definitions updates.

Note: You select Internet-based Scan and Deliver or email-based Scan and Deliver during the Quarantine Server install. To change from one to the other, reinstall the Quarantine Server.

See "Enabling the Quarantine Server" on page 19.

See "Configuring the Quarantine Server" on page 19.

See "Configuring email-based client forwarding" on page 20.

Enabling the Quarantine Server

You configure the Quarantine Server as a centralized repository for infected files that could not be repaired on client computers. Once this is done, you can configure clients to send copies of the files contained in their local Quarantines.

See "Configuring email-based client forwarding" on page 20.

To enable the Quarantine Server

You can enable the Quarantine Server on the local computer and on other computers.

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**, then click **Attach to server.**
2. In the Attach to Quarantine Server dialog box, type the server name, then click **OK**.

To enable the Quarantine Server on another computer

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, 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 part of a domain, type the domain name as well.

See "Configuring the Quarantine Server" on page 19.

See "Configuring email-based client forwarding" on page 20.

Configuring the Quarantine Server

You configure the Quarantine Server as a centralized repository for infected files that could not be repaired on client computers. Email-based Scan and Deliver requires two items of information for Quarantine Server operation:

- The folder location to store files on the Quarantine Server
- The appropriate protocols for your network and the ports on which to listen

Once this is done, you can configure clients to send copies of the files contained in their local Quarantines.

See "Configuring email-based client forwarding" on page 20.

To configure the Quarantine Server

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the General tab, type the Quarantine folder location.
3. Specify the maximum size for the Quarantine.
4. Select the appropriate protocols for your network and specify the port on which to listen.

   Be careful not to use another application's reserved port. Generally, ports over 1025 are not reserved.

See "Enabling the Quarantine Server" on page 19.

Configuring email-based client forwarding

Two types of Central Quarantine clients can forward virus samples to the Quarantine Server:

- Managed, such as Symantec AntiVirus Corporate Edition clients and servers managed with Symantec System Center
- Nonmanaged, such as Symantec AntiVirus for Microsoft Exchange or Symantec AntiVirus for Lotus Notes

A key difference between the two is how virus definitions updates are returned. Under email-based Scan and Deliver, definitions updates are returned by email for all specified platforms and applied under administrator control.

Under Internet-based Scan and Deliver, definitions updates are returned and installed automatically only on computers that are running a managed product. For nonmanaged products, administrators must download and apply updated definitions when notified.

See "Managed and nonmanaged products" on page 39.

To configure client forwarding

You can configure managed and nonmanaged clients to forward to the Quarantine Server.

To configure managed clients to forward to the Quarantine Server

1. In the Symantec System Center Console, in the left pane, right-click a client group, a server group, or server, then click **All Tasks** > **Symantec AntiVirus** > **Quarantine Options**.
2. In the Quarantine Options dialog box, click **Enable Quarantine or Scan And Deliver**.
3. Click **Allow Forwarding To Quarantine Server**.
   By selecting forwarding, clients cannot directly submit items to Symantec Security Response from the Quarantine on the client.
4. For the Server Name, type the server name, IP address, or SPX address of the Quarantine Server.
5. Type the port and protocol that you specified when setting the Quarantine Server properties.
6. Select an automatic operation to run on the client Quarantine when virus definitions updates arrive.

To configure nonmanaged products to forward to the Quarantine Server

1. Locate the Quarantine forwarding settings of the product.
   Refer to the documentation or online Help of the product.
2. Type the server name or IP address where the Quarantine Server is running.
3. Type the port and protocol specified when setting the Quarantine Server properties.

See "Enabling the Quarantine Server" on page 19.

See "Configuring the Quarantine Server" on page 19.

Submitting files for analysis

Quarantine includes the Scan and Deliver Wizard to simplify sending an item to Symantec Security Response for analysis. Your personal data is stripped from the file copies that are sent to Symantec Security Response to ensure your privacy.

Once you receive the definitions update by email, you can apply it first in the Central Quarantine to test and confirm its efficacy. Next, forward the update to the client computer (where the original infected file remains quarantined), which then performs a selected preset operation such as repairing the infected item and releasing it from the client Quarantine automatically.

See "Managing quarantined files" on page 23.

Sending files to Symantec Security Response

The Scan and Deliver Wizard simplifies sending an item to Symantec Security Response for analysis. Scan and Deliver quickly and easily takes only the virus strain (not the entire infected file, for your privacy) and emails it to Symantec for analysis and immediate virus definitions creation.

When you submit an item, the Scan and Deliver Wizard analyzes the file and may recommend an action instead of delivery. For example, the virus may be one that can already be eliminated with your current set of virus definitions. You can override the recommendation and submit it.

Note: You must have an Internet connection and an email address to submit a file to Symantec Security Response.

To submit a file to Symantec Security Response

1. In the Symantec Central Quarantine Console, in the right pane, right-click an item, then click **Submit Item to SARC**.
2. Follow the directions in the Scan and Deliver Wizard to collect information and submit the file to Symantec Security Response for analysis.
3. When the wizard runs, there are two settings to cover special circumstances:
   - Strip File Content: If selected, only the portion of a file that can be infected is sent to Symantec Security Response. Any confidential data and text are stripped from the document before it is submitted. The complete file, however, remains in Quarantine.
   - Specify Custom SMTP Server: This setting applies to corporate environments to route items from the Quarantine to Symantec Security Response through your custom SMTP server.

Managing quarantined files

By default, Symantec and Symantec AntiVirus clients are configured to isolate infected items that cannot be repaired with their current sets of virus definitions. Clients that have been configured to forward these infected files automatically send copies to the Central Quarantine server.

Once these files are in the Central Quarantine, the following administrative actions are possible:

- View a list of quarantined files
- Repair files
- Restore files
- Delete files

See "Submitting files for analysis" on page 22.

See "Viewing a list of quarantined items" on page 24.

See "Deleting quarantined files" on page 25.

See "Repairing and restoring quarantined files" on page 25.

Viewing a list of quarantined items

Files are added to the Central Quarantine when client computers are configured to forward infected items to the Central Quarantine. The information in Table 3-1 is reported.

Table 3-1 Quarantined file information

File information	Description
File Name	Name of the infected item
User Name	User whose file was infected
Computer	Computer where the infected item was discovered
Domain Name	Domain of the infected computer
Received on	When the item was quarantined
Submitted on	When the item was submitted to Symantec Security Response
Submitted by	Who submitted the sample for analysis
Status	Processing state of the sample
Virus	Name of virus identified

To view a list of quarantined items

You can view a list of quarantined items or get detailed information about a quarantined item.

To view a list of quarantined items

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

To get detailed information about a quarantined item

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click an item, then click **Properties**.

See "Submitting files for analysis" on page 22.

See "Deleting quarantined files" on page 25.

See "Repairing and restoring quarantined files" on page 25.

Deleting quarantined files

Although you can delete any item in the Central Quarantine, it is best to reserve this option for files that you no longer need. After confirming that updated definitions detect and eliminate the virus, it is safe to delete the quarantined item.

To delete 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, then click **Delete**.

See "Submitting files for analysis" on page 22.

See "Viewing a list of quarantined items" on page 24.

Repairing and restoring quarantined files

When you choose to restore a file, no attempt is made to repair it. Use this option with discretion to avoid infecting your system. For example, only restore a file 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 their original locations, if possible. If not, you are prompted for a folder location.

When you choose to repair a file, an attempt is made to repair it. You are prompted for a location to store a successful repair. With new virus definitions, you can test the repair in the Central Quarantine before distributing the definitions.

To repair 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, then click **Repair.**

See "Submitting files for analysis" on page 22.

See "Viewing a list of quarantined items" on page 24.

See "Deleting quarantined files" on page 25.

Chapter 4

Using Internet-based Scan and Deliver

This chapter includes the following topics:

About Internet-based Scan and Deliver

Internet-based Scan and Deliver is part of the Digital Immune System, an automated virus sample submission, analysis, and definitions delivery system that provides realtime protection against heuristically detected new viruses.

The Digital Immune System captures files that may be infected with a new virus, and sends them over the Internet to Symantec Security Response. Symantec Security Response collects and automatically analyzes the samples, and if a new virus is found, new virus definitions are automatically produced and returned.

Note: New definitions are packaged as updates to Symantec and Symantec AntiVirus products and distributed immediately to any customer that reports the new virus. The signatures are later distributed to all other customers to prevent the new virus from spreading further.

Enabling and configuring Internet-based Central Quarantine

The Central Quarantine is composed of two components: the Quarantine Server, which is installed on any Windows NT/2000 computer to store infected samples and communicate with Symantec Security Response, and the Quarantine Console that snaps into MMC to perform management tasks.

To use the Central Quarantine, do the following:

- Enable the Quarantine Server.
- Configure the Quarantine Server.
- Configure clients to forward to the Quarantine Server.
- Configure Internet-based Scan and Deliver to transport samples to Symantec Security Response and receive definitions updates.

Note: Internet-based Scan and Deliver or email-based Scan and Deliver is selected during the Quarantine Server install. To change from one to the other, reinstall the Quarantine Server.

See "Enabling the Quarantine Server" on page 29.

See "Configuring the Quarantine Server" on page 30.

See "Configuring Internet-based client forwarding" on page 33.

Enabling the Quarantine Server

You configure the Quarantine Server as a centralized repository for infected files that could not be repaired on client computers. Once this is done, you can configure clients to send copies of the files contained in their local Quarantines.

See "Configuring Internet-based client forwarding" on page 33.

To enable the Quarantine Server

You can enable the Quarantine Server on the local computer and on other computers.

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**, then click **Attach to server**.
2. In the Attach to Quarantine Server dialog box, type the server name, then click **OK**.

To enable the Quarantine Server on another computer

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, 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 part of a domain, type the domain name as well.

See "Configuring the Quarantine Server" on page 30.

See "Configuring Internet-based client forwarding" on page 33.

Configuring the Quarantine Server

Internet-based Scan and Deliver requires two basic items of information for Central Quarantine operation:

- The folder location to store files on the Quarantine Server
- The appropriate protocols for your network and the ports on which to listen

---

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

See "Central Quarantine Properties" on page 31.

See "Enabling the Quarantine Server" on page 29.

See "Configuring Internet-based client forwarding" on page 33.

Configuring the Quarantine

The Quarantine Server receives virus samples from computers running Symantec and Symantec AntiVirus products. The Quarantine Server is the centralized repository for infected files that could not be repaired on client computers.

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

See "Configuring Internet-based client forwarding" on page 33.

To configure the Quarantine Server

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, 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. Specify the maximum size for the Quarantine.
4. Select the appropriate protocols for your network and specify the port on which to listen.

   Be careful not to use another application's reserved port. Generally, ports over 1025 are not reserved.

Central Quarantine Properties

Table 4-1 provides a brief description of the configuration settings available in the Central Quarantine Properties dialog box.

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

Table 4-1 Central Quarantine Properties

Property	Description
General	Basic Quarantine settings, such as the folder location of the Quarantine, maximum size of the folder's contents, listening protocol for communicating with clients, and the console auto-refresh interval.
Web Communication	Communication settings, including the computer name of the Symantec gateway and security settings. ■ Secure submission sends virus samples to Symantec using Secure Socket 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	If you are using a proxy firewall, type the firewall information on this tab. ■ Firewall name is the IP address or 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 4-1 Central Quarantine Properties

Property	Description
Sample Policy	■ 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	■ Active sequence number is the sequence number of the currently installed definitions on the Quarantine Server. Sequence numbers are used only by Symantec AntiVirus Corporate Edition 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.
Install Definitions	■ Install on selected targets (certified definitions) automatically installs certified definitions on the selected servers. Click Select to specify the servers. ■ Install on selected clients (definitions that are not yet certified) automatically installs noncertified definitions on the computers on which the virus was detected. ■ Install on servers of selected clients (definitions that are not yet certified) installs noncertified definitions on the parent server of the infected client. ■ Install on selected targets (definitions that are not yet certified) automatically installs noncertified definitions on the selected servers. Click Select to specify the servers. ■ Delivery Retry interval is, in minutes, how frequently definitions updates are attempted when targets are disconnected. ■ Current Virus Definition File displays the definitions file's version number and date. The version number uses the following conventions: YYMMDDn, where n is the number of the revision, expressed in its alphabetical equivalent.

Table 4-1 Central Quarantine Properties

Property	Description
Customer Information	Displays the customer information you entered during installation. You may change this information, but all fields are required.
Alerting	General settings configure AMS operation. Click Configure to specify the alert mechanism (for example, email, pager, message box, and so on) for each alertable event. Configure Event Notification ■ Event Name enables or disables the alert condition. ■ Timeout (mins) is the amount of time in minutes that the condition must remain true before an alert is sent. Note that for nonmanaged or groupware/gateway clients that do not receive definitions updates automatically, the Cannot install definitions on target machines alert is generated. The alert is posted automatically to the Error tab of the infected item with the locations of FTP sites to download the definitions and the Quarantine Log. If enabled, the Send Internet Mail and Write to Event Log alerts also include this information.
General Errors	Lists the history of Quarantine Server errors.

Configuring Internet-based client forwarding

Two types of Central Quarantine clients can forward virus samples to the Quarantine Server:

- Managed, such as Symantec AntiVirus Corporate Edition clients and servers managed with Symantec System Center
- Nonmanaged, such as Symantec AntiVirus for Microsoft Exchange or Symantec AntiVirus for Lotus Notes

A key difference between the two is how virus definitions updates are returned. Under email-based Scan and Deliver, definitions updates are returned by email for all specified platforms and manually applied under administrator control.

Under Internet-based Scan and Deliver, definitions updates are returned and installed automatically on computers that are running a managed product. For nonmanaged products, administrators must manually download and apply updated definitions when notified.

See "Managed and nonmanaged products" on page 39.

To configure client forwarding

You can configure managed and nonmanaged clients to forward to the Quarantine Server.

To configure managed clients to forward to the Quarantine Server

1. In the Symantec System Center Console, in the right pane, click **All Tasks** > **Symantec AntiVirus** > **Quarantine Options**.
2. In the Quarantine Options dialog box, click **Enable Quarantine or Scan And Deliver.**
3. Click **Allow Forwarding To Quarantine Server.**

   By selecting forwarding, clients cannot directly submit items to Symantec Security Response from the local Quarantine on the client.
4. For the Server Name, type the server name, IP address, or SPX address of the Quarantine Server.
5. Type the port and protocol that you specified when setting the Quarantine Server properties.
6. Select an automatic operation to run on the client Quarantine when virus definitions updates arrive.

To configure nonmanaged products to forward to the Quarantine Server

1. Locate the Quarantine forwarding settings of the product.

   Refer to the documentation or online Help of the product.
2. Type the server name or IP address where the Quarantine Server is running.
3. Type the port and protocol specified when setting the Quarantine Server properties.

See "Enabling the Quarantine Server" on page 29.

See "Configuring the Quarantine Server" on page 30.

Submitting samples for analysis

Sample Policy settings determine whether or not 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.

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

See "Setting an automatic sample submission policy" on page 35.

See "Submitting files manually" on page 35.

Setting an automatic sample submission policy

Sample Policy settings determine whether or not virus samples are submitted automatically to the gateway. If automatic sample submission is not selected, 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: Policy submission settings can be superseded on an item-by-item basis when viewing the Actions tab for a selected item in the Quarantine.

To set sample policy

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

Submitting files manually

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

To be eligible for manual submission:

- 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).

To submit files manually

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

To manually set the priority for a sample

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

To manually submit items 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, then click **All Tasks** > **Queue** item for automatic analysis.

See "Setting an automatic sample submission policy" on page 35.

Managing definitions updates

To manage virus definitions updates, set the following policies:

- Definition Policy: How frequently the Central Quarantine polls the Symantec Security Response gateway for updated, certified definitions
- Install Definitions: Which computers receive certified or noncertified definitions automatically in response to newly discovered viruses from sample submissions

Definitions updates for nonmanaged clients must be downloaded manually.

See "Setting definition policy" on page 37.

See "Installing updated definitions automatically" on page 37.

See "Requesting definitions updates manually" on page 38.

See "Managed and nonmanaged products" on page 39.

Setting definition policy

Definition policy determines how frequently the gateway is polled to download updated certified definitions. Certified definitions are tested by Symantec Security Response before general release.

To set definition policy

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

See "Installing updated definitions automatically" on page 37.

See "Requesting definitions updates manually" on page 38.

See "Managed and nonmanaged products" on page 39.

Installing updated definitions automatically

Install definitions policy determines which computers receive updated definitions automatically in response to virus detections.

Separate policies can be set for certified and noncertified definitions. Certified definitions are tested by Symantec Security Response before distribution. Noncertified definitions are automatically generated by Symantec Security Response in response to a newly discovered virus.

Note: If definitions are delivered for a virus detected on a computer that is not selected to receive definitions automatically, you can manually queue the computer for definitions delivery.

To set install definitions policy

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the Install Definitions tab, set the install definitions policy.

See "Setting definition policy" on page 37.

See "Requesting definitions updates manually" on page 38.

See "Managed and nonmanaged products" on page 39.

Requesting definitions updates manually

A target computer that does not receive definitions updates automatically can be queued for delivery of new definitions. For these computers, the Sample Status is Available. To be eligible for manual definitions delivery:

- The sample cannot already be eligible for automatic delivery of virus definitions (X-Signatures-Priority is 0).
- The sample must require new definitions (X-Signatures-Sequence > 0).
- The sample has not yet been disinfected (X-Date-Finished is missing or 0).

To manually queue a computer for definitions delivery

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click an item, then click **Properties**.
3. In the Properties dialog box, on the Actions tab, click **Queue item for definition delivery**.

   If the item is not eligible for a definitions update, Queue item for definition delivery is not available.

See "Setting definition policy" on page 37.

See "Installing updated definitions automatically" on page 37.

See "Managed and nonmanaged products" on page 39.

Managed and nonmanaged products

Two types of clients can forward items to the Central Quarantine: managed, such as Symantec AntiVirus Corporate Edition clients managed with Symantec System Center, and nonmanaged, such as Symantec AntiVirus for Microsoft Exchange or Symantec AntiVirus for Lotus Notes. The key difference between the two is how the Digital Immune System returns virus definitions updates in response to a newly discovered virus.

- For managed products, definitions created in response to a newly discovered virus are installed automatically.
- Nonmanaged products must be updated manually when definitions are created in response to a newly discovered virus. For these products, an alert is generated that contains the locations of FTP sites from which to download the definitions.

Note: If a nonmanaged product runs under Windows NT/2000, install a managed version of Symantec AntiVirus Corporate Edition on the same computer. Because both Central Quarantine clients share the same set of definitions, the nonmanaged product can forward an infected item to the Central Quarantine and the managed product will receive the definitions update.

Automating virus definitions updates for nonmanaged products

To automate the virus definitions updates for nonmanaged products, you can install Symantec AntiVirus Corporate Edition on the same computer as the nonmanaged product. Because they share the same definitions set, updating Symantec AntiVirus Corporate Edition updates the nonmanaged product as well. This method has the additional benefit of protecting the computer on which the nonmanaged product is installed from virus attack.

When definitions are available for a nonmanaged products, a Cannot install definitions on target machines alert is generated. The alert includes the locations of FTP sites from which to download the definitions.

There are three ways to update virus definitions for nonmanaged products:

- Manually
- With Symantec System Center
- Without using Symantec System Center

Updating definitions manually

When the Central Quarantine receives definitions for a nonmanaged product, a Cannot install definitions on target machines alert is generated. The alert includes the locations of FTP sites from which to download the definitions.

To update definitions manually

To update definitions manually for nonmanaged products, you must locate updated definitions for nonmanaged products and configure an alert that includes FTP locations.

To locate updated definitions for nonmanaged products

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click an item, then click **Properties**.
3. In the Properties dialog box, on the Errors tab, note the FTP sites from which to download updated definitions.

To configure an alert that includes FTP locations

1. In the Symantec Central Quarantine Console, right-click **Symantec Central Quarantine**, then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the Alerting tab, configure a Send Internet Mail or Write to Event Log alert for the Cannot install definitions on target machines event.

   An email is sent or an entry is written to the NT Event Log, respectively.

Updating with Symantec System Center

If Symantec System Center is deployed in the network, updating definitions is straightforward. Simply specify that the Symantec AntiVirus Corporate Edition installed on the same computer as the nonmanaged product receives certified definitions automatically.

To enable definitions updates using Symantec System Center

1. Install Symantec AntiVirus Corporate Edition for servers on the same computer that is running the nonmanaged product.
2. In the Symantec System Center Console, in the left pane, right-click **Symantec Central Quarantine**, then click **Properties**.
3. In the Symantec Central Quarantine Properties dialog box, on the Install Definitions tab, click **Install on selected servers**.
4. Click **Select**, then select the computer running Symantec AntiVirus Corporate Edition.

Updating without using Symantec System Center

If Symantec System Center is not used, you must edit the Registry to enable communication between Symantec AntiVirus Corporate Edition and the Central Quarantine. As a safety precaution, always make a backup copy of the Registry before making any changes.

To update without using Symantec System Center

You can update definitions without using Symantec System Center.

The Symantec AntiVirus Corporate Edition client can also be configured to forward items to the Central Quarantine without using Symantec System Center.

To enable definitions updates without using Symantec System Center

1. On the computer where the Quarantine Server is installed, edit the following Registry key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Quarantine\Server\Avis
2. Change definitionBlessedBroadcast to 1.
3. In definitionBlessedTargets, type the name of the server on which Symantec AntiVirus Corporate Edition is installed.
   To list more than one server, separate each name with a comma.
   Computers can only be identified by name. If the computer's address cannot be resolved from the supplied name, the update will fail. For example, under some circumstances a computer might be addressable only by IP or IPX address.
4. Increment the value of configurationChangeCounter by 1.
   For example, if the value is currently 10, set it to 11.

To enable Symantec AntiVirus Corporate Edition forwarding

1. On the computer where Symantec AntiVirus Corporate Edition is installed, edit the following Registry key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion\Quarantine
2. Change ForwardingEnabled to 1.
3. Set ForwardingPort to the port value that was specified on the General tab when the Symantec Central Quarantine was configured.
   Be sure to enter the port as a decimal value.
4. Set the ForwardingProtocol to one of the following values, as appropriate:
   - 0 for IP
   - 1 for IPX
5. Set ForwardingServer to one of the following, as appropriate:
   - Machine name or IP address for IP
   - <network number>.<node address> for IPX

To locate updated definitions for nonmanaged products

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click the infected item, then click **Properties**.
3. In the Properties dialog box, on the Errors tab, note the FTP sites from which to download updated definitions.

To configure an alert that includes FTP locations

1. In the Symantec Central Quarantine Console, right-click **Symantec Central Quarantine**, then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the Alerting tab, configure a Send Internet Mail or Write to Event Log alert for the Cannot install definitions on target machines event.
   An email is sent or an entry is written to the NT Event Log, respectively.

See "Setting definition policy" on page 37.

See "Installing updated definitions automatically" on page 37.

See "Requesting definitions updates manually" on page 38.

Reviewing sample submission status

A sample's status within the system can be determined by reviewing the actions performed and attributes set during communications between the Quarantine Server and the gateway.

See "Viewing a list of quarantined items" on page 43.

See "Interpreting submission attributes" on page 44.

See "Reviewing actions on samples" on page 45.

See "Reviewing submission errors" on page 45.

Viewing a list of quarantined items

Files are added to the Central Quarantine when client computers are configured to forward infected items to the Quarantine Server. The information in Table 4-2 is reported.

Table 4-2 Quarantined file information

Property	Description
File Name	Name of the infected item
User Name	User whose file was infected
Computer	Computer where the infected item was discovered
Analyzed	Whether the sample was analyzed
Age	How long the sample has been in the Quarantine
Sample State	Analysis state of the sample
Definitions Needed	Sequence number of definitions set to resolve the virus
Sample Status	Processing state of the sample
Virus	Name of virus identified
Sample errors	Sample processing errors

To view a list of quarantined items or to get detailed information about an item

You can view a list of quarantined items and get detailed information about them.

To view a list of quarantined items

- In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
  Quarantined items are listed in the right pane.

To get detailed information about a quarantined item

1. In the Symantec Central Quarantine Console, in the left pane, click **Symantec Central Quarantine**.
2. In the right pane, right-click an item, then click **Properties**.

See "Interpreting submission attributes" on page 44.

See "Reviewing actions on samples" on page 45.

See "Reviewing submission errors" on page 45.

Interpreting submission attributes

Request and response messages exchanged among clients and servers contain numerous attributes that describe a sample completely and its status within the system. 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, then click **Properties**.
3. In the Properties dialog box, on the Sample Attributes tab, double-click a displayed attribute for a brief definition.

See "Sample attributes" on page 57.

See "Viewing a list of quarantined items" on page 43.

See "Reviewing actions on samples" on page 45.

See "Reviewing submission errors" on page 45.

Reviewing actions on samples

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

If desired, 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 view sample actions

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

See "Viewing a list of quarantined items" on page 43.

See "Reviewing submission errors" on page 45.

See "Digital Immune System and Central Quarantine components" on page 9.

Reviewing submission errors

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

To review submission errors

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, then click **Properties**.
3. In the Properties dialog box, on the Errors tab, review submission errors.

See "Viewing a list of quarantined items" on page 43.

See "Interpreting submission attributes" on page 44.

See "Reviewing actions on samples" on page 45.

Sending alerts

In addition to entries in the Quarantine Log, alerts triggered by Central Quarantine events can be sent in the following ways:

- Message box
- Page
- Email
- Broadcast
- NT Event Log entry

Note: For nonmanaged clients that do not receive definitions updates automatically, the Cannot install definitions on target machines alert is generated. The alert is posted automatically to the Error tab of the infected item with the locations of FTP sites from which to download the definitions and the Quarantine Log. If enabled, the Send Internet Mail and Write to Event Log alerts also include this information.

See "Configuring alerting" on page 46.

See "Events that trigger alerts" on page 47.

Configuring alerting

Alert settings determine which events at the Quarantine trigger alerts and where to send them. Alerts for each event can be enabled or disabled individually.

Note: For nonmanaged clients that do not receive definitions updates automatically, the Cannot install definitions on target machines alert is generated. The alert is posted automatically to the Error tab of the infected item with the locations of FTP sites from which to download the definitions and the Quarantine Log. If enabled, the Send Internet Mail and Write to Event Log alerts also include this information.

After identifying the AMS server, specify who receives the alert for each event. After the recipients are configured, each alertable event can be enabled or disabled separately on the Alerting tab.

To configure alerting and specify who receives alerts

You can configure alerting and specify who receives alerts.

To configure alerting

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the Alerting tab, configure alerts.

To specify who receives an alert and by what method

1. In the Symantec Central Quarantine Console, in the left pane, right-click **Symantec Central Quarantine**, then click **Properties**.
2. In the Symantec Central Quarantine Properties dialog box, on the Alerting tab, click **Configure**.
3. Select an event, then click **Configure**.
4. On each panel of the wizard, click **Help** for more information.

See "Events that trigger alerts" on page 47.

Events that trigger alerts

The events listed in Table 4-3 trigger alerts that can be monitored using AMS.

Table 4-3 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 machines	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 will not be forwarded to the gateway.

Table 4-3 Events that trigger alerts

Event	Description
The Quarantine Agent service has stopped	The Quarantine will not be able to 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 noncertified 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 becoming full.
Disk free space is less than Quarantine max size	The Quarantine folder is set to a maximum size greater than the available free disk space.
Sample: was not repaired	Either a sample wasn't repaired or a repair wasn't necessary.
Sample: unable to install definitions	New definitions could not be installed, usually due to a corrupted definitions set.
Sample: processing error	There was an error processing this sample.
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 being 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.
Sample: too long with Submitted status	The sample has not yet been accepted by the gateway.

Table 4-3 Events that trigger alerts

Event	Description
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 being held on the Quarantine Server instead of being delivered.

See "Sending alerts" on page 46.

Appendix A

Sample processing reference

This chapter 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.
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 could not be delivered to the submitting computer.
Quarantined	The sample has been received by the Central Quarantine.
Released	The sample has been queued for analysis.
Restart	Sample processing will begin 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.

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 will 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, and 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. The incorrectly detected infection was caused by a mistake in previous virus definitions files, 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.

Table A-2 Final states

State	Description
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 containing malicious code. The only action you can take on these files is to delete them.
Restore	Files which cannot be cleaned. They may be files altered accidentally or by a virus, and may contain corrupted viral code. Due to the alterations, it is impossible or unsafe to retain the files: You should restored them from a backup.

Transit states

Samples that have not yet reached Symantec Security Response are in one of the transit states. Only components outside Symantec Security Response use the transit states. A sample may remain in a pending state indefinitely before moving to another state. Table A-3 describes the transit states.

Table A-3 Transit states

State	Description
accepted	The sample has been accepted by a gateway, but not yet imported into Symantec Security Response.
importing	The sample is being imported into Symantec Security Response.
receiving	The sample is being received by a gateway.

Pending states

Samples that are awaiting analysis within Symantec Security Response are in one of the pending states. Only components within Symantec Security Response use the pending states. A sample may remain in a pending state indefinitely before moving 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 will be deferred for analysis by experts.
deferred	The sample cannot be analyzed automatically, and has been deferred for analysis by experts.
deferring	The sample cannot be analyzed automatically, and is being 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 moving 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 binary replication.
binaryReplicating	The sample is being executed by a binary replication engine.

Table A-5 Active states

State	Description
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 datatype.
fullBuilding	A new set of virus definitions files incorporating the signatures selected for the new virus are being built.
fullUnitTesting	The full virus definitions files are being unit-tested.
incrBuilding	The signatures 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 spreadsheet containing 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 attributes

Request and response messages exchanged between clients and servers contain numerous attributes in the header that completely describe a sample and its status within the Digital Immune System.

These proprietary attributes are meaningful only to Digital Immune System clients and servers. The attributes always start with the X- characters.

For more information about proprietary attributes, see the following:

- See "X-Analysis attributes" on page 57.
- See "X-Checksum-Method attribute" on page 59.
- See "X-Content attributes" on page 60.
- See "X-Customer attributes" on page 61.
- See "X-Date attributes" on page 63.
- See "X-Error attribute" on page 66.
- See "X-Platform attributes" on page 67.
- See "X-Sample attributes" on page 71.
- See "X-Scan attributes" on page 77.
- See "X-Signatures attributes" on page 79.

X-Analysis attributes

The proprietary X-Analysis attributes are included in messages from Symantec Security Response to gateways, and from gateways to customers, as appropriate. They indicate the current status of a particular sample that has been submitted for analysis.

- See "X-Analysis-Cookie" on page 58.
- See "X-Analysis-Issue" on page 58.
- See "X-Analysis-Service" on page 58.
- See "X-Analysis-State" on page 59.
- See "X-Analysis-Virus-Identifier" on page 59.
- See "X-Analysis-Virus-Name" on page 59.

X-Analysis-Cookie

This attribute contains an arbitrary string assigned by a server when the sample is received. The value has no necessary syntax or meaning, and clients may not interpret the value in any way. Clients store the value returned by the server in a response, and use the value as an argument in subsequent requests for status sent to the same server.

For example, a sample might be assigned this cookie value by a gateway:

- X-Analysis-Cookie: 00000123

X-Analysis-Issue

This attribute contains an arbitrary string assigned by Symantec Security Response for tracking the customer issue when a sample is imported. The value has no necessary syntax or meaning, and clients may not interpret the value in any way. Clients store the value assigned by Symantec Security Response when it is included in a status report, and display the value for customer use when talking to technical support staff.

For example, a sample might be assigned this customer issue tracking value by Symantec Security Response:

- X-Analysis-Issue: 00000042

X-Analysis-Service

This attribute indicates that the results in the status message are from a special class of analysis service. The only supported value is quickcheck for samples that were not fully analyzed.

This value specifies that the sample was not fully analyzed and that the results are not definitive.

For example, the final status message for a sample that is probably not infected with any virus, but has not been definitively found to be uninfected, might include this header:

- X-Analysis-Service: quickcheck

X-Analysis-State

This attribute contains a text token that indicates the current state of the sample. For example, a sample that is currently being transferred from a gateway to Symantec Security Response may be in this state:

- X-Analysis-State: importing

For another example, a sample that has successfully replicated and is ready for the code/data segregation stage may be in this state:

- X-Analysis-State: replicated

Note that state values are not intrinsically final or interim. It is the inclusion of an X-Date-Finished attribute in a status report, not the value of the X-Analysis-State attribute included with it, that indicates that status is final.

X-Analysis-Virus-Identifier

This attribute contains the numerical identifier of a virus found in the sample.

For example, this is the identifier of an especially odd virus:

- X-Analysis-Virus-Identifier: 32767

X-Analysis-Virus-Name

This attribute contains a text string with the name of a virus found in the sample.

For example, this is an especially odd virus:

- X-Analysis-Virus-Name: Morton.42

X-Checksum-Method attribute

The proprietary X-Checksum-Method attribute is included in messages with non-empty content. This attribute tells the receiver what method was used to calculate checksums of the content. The value is the name of the checksum method. The only checksum method used in the Digital Immune System is the Message Digest version 5 (MD5) algorithm, as specified by RFC 1321.

For example, when a message contains a sample, the message will include this attribute:

- X-Checksum-Method: md5

This attribute is omitted if the content of the message is null.

X-Content attributes

The proprietary X-Content attributes are included in messages with non-empty content, as appropriate. These attributes tell the receiver what methods were used to compress, scramble, and encode the message content, if any:

- X-Content-Checksum: MD5 checksum of content
- X-Content-Compression: Method used to compress content
- X-Content-Encoding: Method used to encode content
- X-Content-Scrambling: Method used to scramble content

These attributes are omitted in messages with null content.

X-Content-Checksum

This attribute specifies the MD5 checksum of the content, after any compression, scrambling, or encoding.

For example, the checksum of the content of a message might be:

- X-Content-Checksum: 663E6092463AA20EF6A14E8B137AEF30

This attribute is used to verify that the content has been transferred correctly.

X-Content-Compression

This attribute specifies the method used to compress the content, if any. The value is the name of the compression method. The Digital Immune System uses compression methods defined by the Info-ZIP group.

Table A-6 Compression methods

Value	Description
deflate	For captured samples
zip	For directories of sample analysis files
zip	For directories of signature definitions files

For example, sample submission requests may include this attribute:

- X-Content-Compression: deflate

This attribute is omitted if the content of the message is not compressed.

X-Content-Encoding

This attribute specifies the method used to encode the content, if any. The value is the name of the encoding method. The only method used in the Digital Immune System is the Base64 algorithm, as specified by the Multipurpose Internet Mail Extensions (MIME).

For example, if the content of a message is encoded according to Base64, the message will contain this attribute:

- X-Content-Encoding: base64

This attribute is omitted if the content of the message is not encoded.

X-Content-Scrambling

This attribute specifies the method used to scramble the content, if any. Note that content is scrambled only to prevent accidental execution of potentially infected samples. Scrambling does not provide any security. The value is the name of the scrambling method. The only method used by the Digital Immune System is XOR with a constant bit-mask.

For example, if the content of a message is scrambled, the message will include this attribute:

- X-Content-Scrambling: xor-vampish

This attribute is omitted if the content of the message is not scrambled.

X-Customer attributes

The proprietary X-Customer attributes are included in all messages from customers to gateways. They identify the customer making the request, and are used for authorization and tracking. The names, telephone numbers, and email addresses can be used by the technical support staff to contact the individual who submitted a sample, if necessary.

- X-Customer-Contact-Email: Individual contact information email address
- X-Customer-Contact-Name: Individual contact name
- X-Customer-Contact-Telephone: Individual contact telephone number
- X-Customer-Credentials: Customer authentication information
- X-Customer-Name: Registered name of customer
- X-Customer-Identifier: Customer service class and identifier

X-Customer-Contact-Email

This attribute gives individual contact information. The value is a text string of at most 255 characters giving the email address that the technical support staff can use to contact the individual who submitted a sample, if necessary.

For example, the contact information might be:

- X-Customer-Contact-Email: someone@symantec.com

X-Customer-Contact-Name

This attribute gives individual contact information. The value is a text string of at most 255 characters giving the full name of an individual that the technical support staff can contact, if necessary.

For example, the contact information might be:

- X-Customer-Contact-Name: Jim Hill

X-Customer-Contact-Telephone

This attribute gives individual contact information. The value is a text string of at most 255 characters giving the telephone number of an individual that the technical support staff can contact, if necessary.

For example, the contact information might be:

- X-Customer-Contact-Telephone: 310-555-1212

X-Customer-Credentials

This attribute transports customer credentials from a customer client to a gateway. The value is used by the gateway when a sample is received.

For example, the customer credentials might be:

- X-Customer-Credentials:
  0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF

X-Customer-Name

This attribute gives the registered name of the customer. The value is a text string of at most 255 characters giving the name of the person and organization that purchased the product or subscribed to the service.

For example, the customer name might be:

- X-Customer-Name: Jim Hill, Symantec Corp

X-Customer-Identifier

This attribute specifies the customer's service class and identification number. The value is a text string of at most 63 characters.

The value is assigned when a customer installs a product or subscribes to a network service.

The service class is indicated by one of the text tokens listed in Table A-7.

Table A-7 Service classes

Class	Description
gold	For the gold service plan
platinum	For the platinum service plan

For example, the customer identifier for the author might be:

- X-Customer-Identifier: 123456-ABCDEFgold 0123456789ABCDEFGHIJ

X-Date attributes

The proprietary X-Date attributes are included in all messages, as appropriate. They record the date and time of significant events in the processing of samples or signatures. They include, but are not limited to:

- X-Date-Accessed: When the file was last accessed
- X-Date-Analyzed: When the sample was analyzed
- X-Date-Blessed: When the signatures were blessed
- X-Date-Captured: When the sample was captured
- X-Date-Created: When the file was created
- X-Date-Distributed: When the signatures were scheduled for delivery
- X-Date-Finished: When the sample analysis was finished
- X-Date-Forwarded: When the sample was forwarded to the Quarantine
- X-Date-Installed: When the signatures were installed
- X-Date-Modified: When the file was modified
- X-Date-Produced: When the signatures were produced in the back office

- X-Date-Published: When the signatures were produced/published on the Internet
- X-Date-Submitted: When the sample was submitted for analysis

The value specifies the time and date of an event according to the sender's system clock, expressed as Greenwich Mean Time (GMT) in the format defined in RFC 1945 and RFC 822.

For example, the value of this attribute for this document is:

- X-Date-Created: Tue, 27 Jan 1998 14:32:45 GMT

When a message reception begins, the difference between the sender's and receiver's clocks is calculated by comparing the value of the Date attribute received with the local clock. The timestamp values stored are relative to the local clock.

X-Date-Accessed

This attribute is included when a message contains a sample or a signature set. The value is the date and time that the file in the message content was last accessed.

X-Date-Analyzed

This attribute is included with status about a sample. The value is the date and time when the sample was analyzed.

X-Date-Blessed

This attribute is included when the message refers to a signature set that has been blessed. The value is the date and time when the signatures were published on the Internet. When this attribute is included in a message, the signatures have been fully tested and supersede all previous signatures.

X-Date-Captured

This attribute is included when a message contains a sample. The value is the date and time when the sample was originally captured.

X-Date-Created

This attribute is included when a message contains a sample or a signature set. The value is the date and time that the file in the message content was created.

X-Date-Distributed

This attribute is included when the message refers to a signature set that has been scheduled for delivery to an infected workstation. The value is the date and time that the delivery was scheduled.

X-Date-Finished

This attribute is included with status about a sample. The value is the date and time when analysis of the sample was finished. When this attribute is included in a message, the status attributes in the message are final.

X-Date-Forwarded

This attribute is included when a message refers to a sample that has been forwarded to Quarantine. The value is the date and time when the sample was quarantined.

X-Date-Installed

This attribute is included when the message refers to a signature set that has been installed on an infected workstation. The value is the date and time that the signatures were installed.

X-Date-Modified

This attribute is included when a message contains a sample or a signature set. The value is the date and time that the file in the message content was last modified.

X-Date-Produced

This attribute is included when the message contains a signature set. The value is the date and time when the signatures were produced in the back office.

X-Date-Published

This attribute is included when the message contains a signature set. The value is the date and time when the signatures were published on the Internet.

X-Date-Submitted

This attribute is included when a message refers to a sample that has been submitted for analysis. The value is the date and time when the sample was sent to an Internet gateway.

X-Error attribute

The proprietary X-Error attribute is included in response messages when requests cannot be processed correctly. They describe the reason that the request could not be processed, and may optionally include parameters that further qualify the error.

X-Error: error code and optional parameters

For example, a server that is unable to process a signature download request for a set of signatures named 12345 because they are no longer available might include this header in its response:

- X-Error: superseded

A server that is unable to process a sample submission request because the value of the Content-Length header does not match the size of the message content might include this header in its response:

- X-Error: overrun 10138 10139

Table A-8 lists the error codes.

Table A-8 Error codes

Code	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 cookie has not been assigned by the gateway.
declined	The sample submitted for analysis has been declined by the gateway. This may be due to invalid service subscriber identification. 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 may be due to a transmission error in the transport network.
sample	The sample's sample checksum does not match its content.

Table A-8 Error codes

Code	Description
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 could not be unpacked.
unpublished	The signature set could not be published.

X-Platform attributes

The proprietary X-Platform attributes are included in all messages that contain samples. They describe the hardware and software of the computer that captured the sample.

- X-Platform-Address: List of IP and IPX addresses
- X-Platform-Correlator: Unique correlator
- X-Platform-Distributor: Network name of distribution server
- X-Platform-Domain: Name of administrative domain
- X-Platform-GUID: Unique identifier for managed client computers
- X-Platform-Host: Network name of computer
- X-Platform-Language: National language of operating system
- X-Platform-Owner: Registered owner and organization
- X-Platform-Processor: Processor vendor make and model and clock rate
- X-Platform-QServer-CountryCode: IBM country code of the Quarantine Server computer
- X-Platform-QServer-WinINet: Version of Wininet.dll
- X-Platform-QServer-WinINet-Encryption: Encyption level supported by the WinINet version
- X-Platform-Scanner: Antivirus vendor, product, and version

- X-Platform-System: Operating system vendor and version
- X-Platform-User: Network name of logged-on user

X-Platform-Address

This attribute specifies the IP and IPX addresses of the computer that captured the sample. The value is a list of numeric IP addresses and IPX addresses, separated by blanks.

For example, the address of the author's workstation is:

- X-Platform-Address: 9.2.18.13

When a computer has multiple IP addresses and/or multiple NetBIOS addresses, all addresses are included in the value. This is particularly common for servers.

X-Platform-Correlator

This attribute specifies a value that correlates all samples submitted from a particular platform. The value is a text string of at most 32 bytes.

The value is arbitrary and unique for each possible platform. The value is used to correlate samples submitted from the same platform for the purpose of limiting the number of samples a particular platform can submit. The value is not used to identify the platform, individual, or customer.

For example, the correlator assigned to the author's workstation is:

- X-Platform-Correlator: 0123456789ABCDEF0123456789ABCDEF

X-Platform-Distributor

This attribute specifies the network name of the distribution server from which the computer obtains signature updates. The value is a string specifying the network name of the computer hosting the distribution service.

For example, the distribution service for a workstation might be:

- X-Platform-Distributor: AVFILES

This attribute is omitted if no administration domain is available.

X-Platform-Domain

This attribute specifies the administrative domain of the computer that captured the sample. The value is a string specifying the LANDesk administration domain to which the computer that captured the sample belongs.

For example, the administration domain might be:

- X-Platform-Domain: AVBUILD

This attribute is omitted if no administration domain is available.

X-Platform-GUID

This attribute specifies a unique identifier for a client computer assigned by a network management application. The value is a text representation of a globally unique identifier (GUID) stripped of all punctuation characters.

For example, a network management application might assign this identifier to a client computer:

- X-Platform-GUID: 0123456789ABCDEF0123456789ABCDEF

This attribute is omitted if the computer is not a managed client.

X-Platform-Host

This attribute specifies the network identity of the computer that captured the sample. The value is a fully qualified TCP/IP name or a NetBIOS name.

For example, the TCP/IP name might be:

- X-Platform-Host: someone.symantec.com

This attribute is omitted if no TCP/IP or NetBIOS host name is available.

X-Platform-Language

This attribute specifies the national language of the computer that captured the sample. The value is a text string identifying the national language and locale.

For example, the national language and locale for United States English is:

- X-Platform-Language: English (United States)

X-Platform-Owner

This attribute specifies the owner of the computer that captured the sample. The value is a string naming the owner and organization.

For example, the registered owner of the author's workstation, as recorded in its registry at SOFTWARE\Microsoft\WindowsNT\CurrentVersion, might be:

- X-Platform-Owner: Jim Hill, Symantec Corp

X-Platform-Processor

This attribute describes the processor in the computer that captured the sample. The value is a string naming the vendor make and model and clock rate of the processor.

For example, the processor, as recorded in its registry at HARDWARE\DESCRIPTION\System\CentralProcessor\0, might be:

- X-Platform-Processor: Genuine Intel 165 MHz x86 Family 5 Model 2 Stepping 12

X-Platform-QServer-CountryCode

This attribute specifies the IBM country code of the computer that the Quarantine Server is running on. The country code is based on international phone codes, also referred to as IBM country/region codes.

For example, the country code might be:

- X-Platform-QServer-CountryCode: 1

X-Platform-QServer-WinINet

This attribute specifies the version of the WinINet installed on the Quarantine Server.

For example, the version of WinINet installed might be:

- X-Platform-QServer-WinINet: 5.00.2614.3400

X-Platform-QServer-WinINet-Encryption

This attribute specifies the encryption level used by Internet Explorer installed on the computer that the Quarantine Server is running on. It will be either 40 or 128 bits.

For example, the encryption level might be:

- X-Platform-QServer-WinINet-Encryption:128

X-Platform-Scanner

This attribute describes the antivirus protection in the computer that captured the sample. The value is a string naming the vendor and version and signature sequence number of the antivirus product.

For example, the antivirus protection installed on a workstation might be:

- X-Platform-Scanner: Symantec AntiVirus for Windows version 5.0

X-Platform-System

This attribute describes the operating system in the computer that captured the sample. The value is a string naming the vendor and version of the operating system and version.

For example, the operating system installed on the author's workstation, as recorded in its registry at SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ is:

- X-Platform-System: Windows NT 4.0 build 1381 Service Pack 3

X-Platform-User

This attribute specifies the network identity of the user logged onto the computer that captured the sample. The value is a string specifying the user's Windows or NetBIOS logon name.

For example, the author's NetBIOS logon name is:

- X-Platform-User: PRING

This attribute is omitted if no Windows or NetBIOS logon name is available.

X-Sample attributes

The proprietary X-Sample attributes are included in all messages that contain samples. They describe the sample as follows:

- X-Sample-Changes: Attribute change indicator in Quarantine
- X-Sample-Checksum: MD5 checksum of captured data
- X-Sample-Checkup: Checkup database entry for file samples
- X-Sample-Extension: Extension for file samples
- X-Sample-File: Drive and directory and name for file samples
- X-Sample-Geometry: Cylinder and head and sector numbers and size
- X-Sample-Priority: Queuing priority

- X-Sample-Reason: Reason for capturing the sample
- X-Sample-Sector: Disk address numbers of sector samples
- X-Sample-Service: Name of requested service
- X-Sample-Size: Size of captured data
- X-Sample-Status: Status of sample in Quarantine
- X-Sample-Strip: Method used to remove user data
- X-Sample-Switches: Undocumented processing switches
- X-Sample-Type: Type of sample

X-Sample-Changes

This attribute is included in all messages that contain samples. This attribute indicates that one or more other attributes have changed while the sample was stored in the sample queue of a Quarantine service. The value is an integer that is incremented after new attributes are added, or the values of existing attributes are changed. The value itself is not significant; the fact that it has changed indicates that the values of other attributes must be re-examined for significant changes.

For example, after a sample is captured and a Quarantine agent has added its initial attributes, the sample may include this attribute:

- X-Sample-Changes: 1

For another example, after a sample is forwarded to a Quarantine server and it has added more attributes, the sample may include this attribute:

- X-Sample-Changes: 2

X-Sample-Checksum

This attribute specifies the MD5 checksum of the data that was captured, before any compression or scrambling or encoding.

For example, the MD5 checksum for a sample might resemble:

- X-Sample-Checksum: 8B37247C71443D40A2D7FCF16867803A

This attribute is used to detect duplicates, and to validate unscrambling and decompression.

X-Sample-Checkup

This attribute is included in messages that contain samples, when available. It contains the checkup database entry for the file from the computer that captured

the sample. This information, stored before the sample was infected, is useful in analyzing the virus and testing the repair instructions.

For example, a typical checkup database entry might be:

- X-Sample-Checkup: 0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF012345678

If there is no entry in the checkup database for a file when a sample of it is captured, this attribute is omitted.

X-Sample-Extension

This attribute specifies the extension of the file that was captured, for file samples. The value is the extension only, without the drive or directory or name or period (.) character.

For example, the extension of a file sample might be:

- X-Sample-Extension: doc

This attribute is redundant, since the extension of a file sample is included in the X-Sample-File attribute. This redundancy is necessary because the X-Sample-File attribute may be removed from a sample before submission, along with other sensitive user data.

X-Sample-File

This attribute specifies the file that was captured, for file samples. The value is the drive and directory and name of the file captured.

For example, the drive and directory and name of a file sample might be:

- X-Sample-File: C:\Memos\December.doc

X-Sample-Geometry

This attribute specifies the geometry of a disk. The number of cylinders and heads and sectors are specified as three decimal numbers, separated by slash characters, and the number of bytes per sector is specified as a decimal number.

For example, the geometry of a disk might be:

- X-Sample-Geometry: 80/2/18 chs 512 bytes

For another example, the geometry of a disk drive might be:

- X-Sample-Geometry: 800/8/32 chs 512 bytes

X-Sample-Priority

This attribute specifies the queuing priority of the sample. The value is an unsigned integer in the range 0 to 1000. This value represents the importance of the sample, relative to other samples in the same queue, and determines the order in which samples are processed at queuing points. Larger values indicate higher priority, and smaller values indicate lower priority.

For example, the priority of an unimportant sample might be:

- X-Sample-Priority: 1

For another example, the priority of a more important sample might be:

- X-Sample-Priority: 999

X-Sample-Reason

This attribute specifies the reason for capturing the sample. The value is a text token that indicates why the sample was captured. Table A-9 describes the sample reasons.

Table A-9 Sample reasons

Reason	Description
badrepair	When repair for a known virus failed
manual	When the sample was captured manually by a user
norepair	When repair for a known virus was unavailable
suspicious	When the sample contains code similar to a known virus
variant	When the sample has a new variant of a known virus

For example, a sample may be captured because it is infected with a new virus that is similar to a known virus:

- X-Sample-Reason: variant

For another example, a sample may be captured because repair for a known virus was unsuccessful:

- X-Sample-Reason: badrepair

X-Sample-Sector

This attribute specifies the disk addresses that were captured, for sector samples. The value is a list of one or more sector addresses. Sector addresses are encoded as three decimal numbers, separated by slash characters, specifying cylinder number

and head number and sector number. The sectors captured may be specified individually or as a range. A range of sectors is encoded as a starting sector address and an ending sector address, separated by a hyphen character.

For example, the addresses of a sample of an entire disk might be:

- X-Sample-Sector: 0/0/0-79/1/17

For another example, the addresses of a sample of the first track and the last sector on a disk drive might be:

- X-Sample-Sector: 0/0/0-0/0/31 799/7/31

X-Sample-Service

This attribute requests a special class of analysis service. The only supported value is quickcheck for samples likely to be uninfected.

This value specifies that the sample is not entitled to the full analysis service that samples receive by default. Such samples may not be fully analyzed, and the results returned may not be definitive. An X-Analysis-Service attribute will be included with final status if the results are not definitive.

For example, a sample captured manually by a consumer might include this header:

- X-Sample-Service: quickcheck

X-Sample-Size

This attribute specifies the size of the data that was captured, before any compression or scrambling or encoding. The value is a decimal number of bytes.

For example, the size of a file sample of a large document might be:

- X-Sample-Size: 12345678

X-Sample-Status

This attribute specifies the status of a sample while in the sample queue of a Quarantine service. The value is a text token that indicates the current status of the sample. Table A-10 describes the sample statuses.

Table A-10 Sample statuses

Status	Description
available	When new signatures are available
distributed	When new signatures have been distributed

Table A-10 Sample statuses

Status	Description
held	When the sample is withheld from submission
installed	When new signatures have been installed
needed	When new signatures are needed
released	When the sample has been released for submission
submitted	When the sample has been submitted for analysis
unneeded	When new signatures are not needed

For example, a sample that has not yet been submitted for analysis may have this status:

- X-Sample-Status: held

For another example, a sample that has been analyzed and found to be infected with a new virus may have this status:

- X-Sample-Status: available

X-Sample-Strip

This attribute specifies the method used to remove user data from the sample. The value is the name of the stripping method. User data may be removed from a sample when it is captured or at any time thereafter. In any case, when user data is removed from a sample, the values of attributes such as X-Sample-Checksum and X-Sample-Size reflect the content of the stripped sample that has been submitted for analysis, not the original user file.

For example, if user data has been stripped from a sample by over-writing it with binary zeroes, the message might include this attribute:

- X-Sample-Strip: overwrite-zeroes

This attribute is omitted if user data has not been removed from the sample.

X-Sample-Switches

This attribute specifies undocumented switches that affect the processing of a sample within Symantec Security Response. The value is one or more tokens separated by blanks.

X-Sample-Type

This attribute specifies the type of sample that was captured. Table A-11 describes sample types.

Table A-11 Sample types

Type	Description
file	For file samples
sector	For sector samples

For example, the type of sector sample of an entire disk might be:

- X-Sample-Type: sector

X-Scan attributes

The proprietary X-Scan attributes are included in all messages that contain samples. They describe the results of scanning the sample for known viruses with the latest signatures available.

- X-Scan-Result: Result of scanning sample
- X-Scan-Signatures-Name: Name of signatures with which sample was scanned
- X-Scan-Signatures-Sequence: Sequence number of signatures for the scan
- X-Scan-Signatures-Version: Daily version number of signatures
- X-Scan-Virus-Identifier: Identifier of the virus found
- X-Scan-Virus-Name: Name of the virus found

X-Scan-Result

This attribute specifies the result of scanning the sample. Table A-12 describes the scan results.

Table A-12 Scan results

Result	Description
badrepair	A repair engine failed.
badscan	A scan engine failed.
completed	The virus was scanned but the result is not available.

Table A-12 Scan results

Result	Description
heuristic	The sample may contain a new virus.
nodetect	The sample does not contain any known viruses.
norepair	The virus infecting a sample cannot be safely removed.
overrun	A repair engine wrote outside a sample buffer.
repaired	The virus infecting a sample can be removed.
underrun	A repair engine wrote outside a sample buffer.
unrepairable	The virus infecting a sample cannot be removed.
unsubmittable	The sample is probably a Trojan horse.

For example, if a sample may be infected with a variant of a new virus, but the virus cannot be verified, the result may be:

- X-Scan-Result: heuristic

X-Scan-Signatures-Name

This attribute specifies the name of the signatures used to scan the sample.

For example, the name of a full set of virus signature definitions files for Windows 95/98/NT products might resemble:

- X-Scan-Signatures-Name: 00000678.all.zip

X-Scan-Signatures-Sequence

This attribute specifies the sequence number of the signatures used to scan the sample.

For example, the sequence number of virus signature definitions files might resemble:

- X-Scan-Signatures-Sequence: 00000678

X-Scan-Signatures-Version

This attribute specifies the daily version number of virus signature definitions files that are used to scan the file.

For example:

- X-Scan-Signatures-Version: 1999.02.06.001

X-Scan-Virus-Identifier

This attribute contains the identifier of a virus found in the sample.

For example:

- X-Scan-Virus-Identifier: 32767

X-Scan-Virus-Name

This attribute specifies the name of the virus found in the sample.

For example:

- X-Scan-Virus-Name: Morton.42

X-Signatures attributes

The proprietary X-Signatures attributes are included in all messages that contain or refer to virus signature definitions files. They identify sets of signatures produced by the back office.

- X-Signatures-Checksum: MD5 checksum of definition package
- X-Signatures-Priority: Queuing priority
- X-Signatures-Sequence: Sequence number of signature set
- X-Signatures-Version: Daily version number of signature set

X-Signatures-Checksum

This attribute specifies the name of a full set of MD5 checksum of the package containing the virus signature definitions files.

For example, the name of an all-products definition MD5 checksum for a package might resemble:

- X-Signatures-Checksum: 8B37247C71443D40A2D7FCF16867803A

X-Signatures-Priority

This attribute specifies the queuing priority of the signatures. The value is an unsigned integer in the range 0 to 1000, with larger values indicating higher priority and smaller values indicating lower priority.

For example, the priority of unimportant signatures might be:

- X-Signatures-Priority: 0

For another example, the priority of more important signatures might be:

- X-Signatures-Priority: 1

X-Signatures-Sequence

This attribute specifies the sequence number of virus signature definitions files.

For example, the sequence number of a set might resemble:

- X-Signatures-Sequence: 00000678

X-Signatures-Version

This attribute specifies the daily version number of virus signature definitions files.

For example, the daily version number of a signature set might resemble:

- X-Signatures-Version: 1999.02.06.001

Sample errors

Sample processing errors include those listed in Table A-13.

Table A-13 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 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 may be due to a transmission error in the transport network.
sample	The sample's sample checksum does not match its content.

Table A-13 Sample errors

Error	Description
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 could not be unpacked.
unpublished	The signature set could not be published.

Index

F

G

H

I

L

M

N

P

Q

S

V

W

X