Using the Configuration Editor tool

This document provides the information you need to set configuration options for your Symantec antivirus protection using the Configuration Editor tool. It includes the following topics:

Introducing the Configuration Editor tool

The configurations file (Grc.dat) is the heart of the communication between the following:

- Symantec Client Security antivirus server and client
- Symantec AntiVirus Corporate Edition server and client

Configuration files store important information, such as parent server identity and antivirus server and client configuration settings.

You can use the Configuration Editor (Configed.exe) to generate a configurations file that can be used with Symantec Client Security antivirus server and client or Symantec AntiVirus Corporate Edition server and client.

Using the Configuration Editor, you can create various configurations that can be distributed to antivirus clients at any time. For example, an administrator of an organization with separate server groups that are set up for departments with different security needs can create a configuration file with different settings for each of the server groups.

Note: Creating Grcgrp.dat and Grcgrpl.dat files with the Configuration Editor is not supported.

Getting started with the Configuration Editor

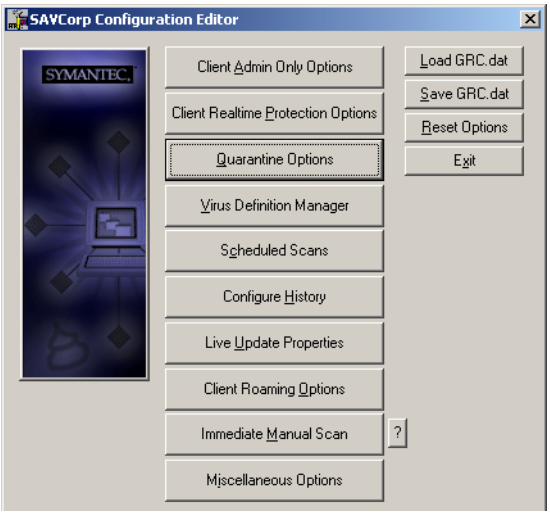
To start using the Configuration Editor, you need to copy the program from the installation CD onto your desktop. You can then launch it.

To copy the Configuration Editor onto the desktop

1. Insert the installation CD into your CD ROM drive.
2. Open **Tools** > **Nosuprt** > **Configed**.
3. Copy Configed.exe to your Windows desktop.

To launch the Configuration Editor

- On the Windows desktop, double-click the Configed icon.



Creating or modifying a configurations file

You can set options with the Configuration Editor and create a new configurations file or load an existing Grc.dat to edit.

To create a configurations file, you complete the following tasks:

- Set configuration options.
- Save the file.

To modify a configurations file, you complete the following tasks:

- Load a configurations file.
- Set configuration options.
- Save the file.

To load a configurations file

1. In the main Configuration Editor window, click **Load GRC.dat**.
2. Locate and load the configurations file.

Saving a configurations file

You can save the configurations file that you create either as Grc.dat (the default name) or with a name that you specify. Before you roll out the configurations file, it must be renamed to Grc.dat.

To save a configurations file

1. In the main Configuration Editor window, click **Save GRC.dat**.
2. Locate the directory to which you want to save the file.
3. Do one of the following:
   - Accept grc as the name of the .dat file.
   - Type a new name in the File Name text box.
4. Click **Save**.

   The file must be named Grc.dat and placed in the appropriate directory before it will be processed:
   - For Windows 98\Me: C:\Program Files\Norton AntiVirus
   - For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
   - For Windows 2000\XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5

Returning settings to their default configuration

At any time while you are creating or editing a Grc.dat, you can return all settings to their defaults.

To return all settings to their default configuration

- In the main Configuration Editor window, click **Reset Options**.

Setting administrator-defined client options

You can set client options on the primary server for your server group. All connected clients will use these settings when they are not superseded by settings set at the client group or individual client level.

Table 1-1 Client Admin Only Options: General controls

Option	Description
Show Norton AntiVirus icon on desktop	By default, the antivirus program icon does not appear in the Windows taskbar on the client computer. To make the icon appear, enable Show Norton AntiVirus icon on desktop.
Display message when definitions are outdated	When the antivirus program detects a virus, you can notify the user of the problem by displaying a warning message on the infected computer's screen.
Warn after ___ days	The number of days at which you want to be warned. The default is 90.
Warning Message	You can customize the warning message displayed on the client computer, depending upon your virus protection strategy; for example, you could display a message explaining how to update definitions.
Snooze scheduled scans when running on batteries	If the antivirus program determines that the computer is running on batteries, the scan will be snoozed. (The snooze lasts for one or three hours, depending on the snooze configuration settings. The number of snoozes allowed is also part of the snooze configuration settings.)
Lock the ability of users to unload Norton AntiVirus Services	When enabled, prevents users from disabling or removing the antivirus program or scanning mapped network drives. This option is enabled by default.
Ask for password to allow uninstall of Norton AntiVirus client	When enabled, prevents users from uninstalling the antivirus program unless they know a specified password. This option is enabled by default.
Change	Use to set the password.
Ask for password to scan a mapped network drive	If enabled, users cannot initiate a scan of mapped network drives unless they know the password. This option is enabled by default.
Change	Use to set the password.

Locking realtime protection options

Locking realtime protection options works as follows:

- If you configure and lock a client realtime protection option at the server group or server level, connected client computers read and use the new configuration from the server to which they connect.
- If you configure but do not lock a client realtime protection option at the server group or server level, the currently connected client computers do not read or use the new server or server group configuration. These changes will be propagated to future client installations.
- If you select multiple clients for a server and the clients have different realtime protection options, a question mark (?) is displayed over the Lock button. When you lock or unlock the setting, the change is propagated to the selected clients.

Setting options for file system, Lotus Notes, and Microsoft Exchange realtime protection

You can set options that determine how the antivirus program handles the problems that it finds.

You can set realtime protection options for:

- File system
- Lotus Notes
- Microsoft Exchange

Table 1-2 Options for file system, Lotus Notes, and Microsoft Exchange realtime protection

Option	Description
Enable file system realtime protection	Lets realtime scans inspect files for known viruses on a continuous basis as the files are read from or written to a computer.
Advanced	Opens the Scan Advanced Options dialog box where you can specify in greater detail how a scan is executed.
All Types	Click to scan all files.
Selected Extensions	Click to select the file type extensions that you want to include in the scan.

Table 1-2 Options for file system, Lotus Notes, and Microsoft Exchange realtime protection

Option	Description
Selected Types	Click to select the file types you want to include in the scan. This option is for Windows 3.1x clients.
Macro Virus and Non-Macro Virus Tabs	
Action	Select the action to take when a macro virus is encountered.
If action fails	Select the action to take if the primary action fails when a macro virus is encountered.
Clean virus from file	The antivirus program attempts to clean an infected file as soon as a virus is detected. This is the default setting.
Quarantine infected file	The antivirus program attempts to move the infected file to Quarantine on the infected computer as soon as a virus is detected. After an infected file is moved to Quarantine, you cannot execute it until you take an action (for example, clean or delete) and move the file back to its original location.
Delete infected file	The antivirus program attempts to delete the file. Use this option only if you can replace the infected file with a virus-free backup copy because the file is permanently deleted and cannot be recovered from the Recycle Bin.
Leave alone (log only)	The antivirus program notifies you of the virus and logs the event but does not perform any other action. If you prefer to control how a virus is handled, click the Leave alone (log only) option. When you are notified of the virus, right-click the file name in Virus History, and click one of the following actions: Clean, Delete Permanently, or Move To Quarantine.
Display message on infected computer	When the antivirus program detects a virus, you can notify the user of the problem by displaying a warning message on the infected computer's screen.

Table 1-2 Options for file system, Lotus Notes, and Microsoft Exchange realtime protection

Option	Description
Message	Opens the Display Message dialog box where you can create a message. The default message uses message parameters to display pertinent information about the infection on your computer. When displayed on a computer, the message might look like this: Scan type: Scheduled Scan Event: Virus Found Stoned-C File: C:\AUTOEXEC.BAT Location: C: Computer: JSMITH-2 User: JSmith Action taken: Cleaned You can change this message by entering new text or adding message parameters—information placeholders containing changing data.
Exclude selected files and folders	You can specify which files you want to exclude from scanning, using file type extensions as the criterion. You can also specify which folders and drives you want to exclude.
Floppy, Network, or CD-ROM	The network drive option applies to all computers. The floppy disk and CD-ROM drive options apply only to Windows 3.x computers. If you are configuring protection for computers running Windows 9x/NT/2000/Me/XP or NetWare, these options do not apply.
Network	If enabled, the antivirus program scans files as they are written from a client computer to a server (or from a server to another server). This option is not necessary if you enable realtime protection on your servers. For example, suppose that you enable scanning of network drives on Client A and also have realtime protection enabled on Server B. When Client A writes a file to a network drive on Server B, the antivirus program scans the file on Client A and then scans the file again on Server B. This could reduce network performance on the client computer.
Floppy	If enabled, the antivirus program scans files as they are read from or written to floppy disks. Floppy disks are common sources of virus infections because users may bring infected disks from home.
CD-ROM	On occasion, some software companies ship CD-ROMs with infected files on them.

Table 1-2 Options for file system, Lotus Notes, and Microsoft Exchange realtime protection

Option	Description
Lock buttons	Click the lock button to display a closed lock which prevents users on client computers from changing that setting. Only locked options are changed on clients.
Insert warning into e-mail message	Symantec AntiVirus can insert a warning message into the body of an email message associated with an infected attachment. Therefore, if you receive an infected attachment, you will be warned when you read the email message. This type of warning can be important if Symantec AntiVirus is unable to clean the virus from the email attachment, and the attachment file is moved, left alone, deleted, or renamed. The warning message tells you which virus was found and explains what action was taken against the infection.
Send e-mail to sender	You can stop a serious virus outbreak before it starts by notifying the sender about an infected file. You can set up Lotus Notes, or Microsoft Exchange Realtime Protection to automatically notify the sender of an infected email attachment via email.
Send e-mail to selected:	Sends email notifying others about a virus infection. After you enter the names of the individuals to be notified, Symantec AntiVirus sends an email message containing information about the virus infection to the people on your list.

Setting file system realtime protection advanced options

File system advanced realtime protection options determine the file operations that realtime protection monitors.

Table 1-3 File system realtime protection advanced options

Option	Description
Modified (scan on create)	Checks for viruses in files that have been created, written to, modified, renamed, or moved. This permits faster performance because the number of file processes that realtime protection monitors is limited.
Accessed or modified (scan on create, open, move, copy, or run)	Checks files that are created, modified, opened, executed, copied, or saved. This results in slower performance than does the previous option but is more thorough, so it provides better protection against viruses. This option is enabled by default.

Table 1-3 File system realtime protection advanced options

Option	Description
Opened for backup	For computers that are running Windows NT/2000/XP, scans files that are accessed during a backup operation. Use this option if you haven't run a virus check on files that you want to back up. Using this option can significantly slow backup operations, since realtime protection scans each file that is included in the back up.
When realtime protection is disabled, enable after ____ Minutes	When realtime protection has been disabled, automatically reenables it after the specified number of minutes.
Back up before attempting repair	As a data safety precaution, the antivirus program makes a backup copy of a file before attempting to repair it by default. The backup copy is stored in the Quarantine directory. (The antivirus server for NetWare does not support this option.)
Heuristics	Lets you change the level of protection provided by Bloodhound Heuristic Scanning. Bloodhound can detect a high percentage of unknown viruses by isolating and locating the logical regions of a file. Bloodhound then analyzes the program logic for virus-like behavior.
Floppies	Lets you to change the current setting for floppy disk scanning.
Check floppies for boot viruses upon access	The antivirus program scans the floppy disk in the floppy drive for a boot virus when the drive is first accessed. When a boot virus is found, you must select whether to clean a virus from the boot record or leave it alone. If you select Leave alone (log only), an alert is sent when a virus is detected but no action is taken. Use this option if you want to take direct control over the virus cleaning and handling process. For example, after you receive the alert, you can decide what course of action to take.
Do not check floppies upon system shutdown	The antivirus program skips the scan of any floppy disk in the floppy drive when the computer is shut down normally.

Table 1-3 File system realtime protection advanced options

Option	Description
Monitor (Windows 9x only)	Disables protection monitors for virus-like activities. Virus-like activities are activities that viruses perform when attempting to infect your files. Any of these activities might occasionally be legitimate in your work context. The following activities can be excluded from monitoring: ■ Low-Level Format Of Hard Disk: All information on the drive is erased and cannot be recovered. This type of format is generally performed at the factory only. If this activity is detected, it usually indicates an unknown virus at work. (This is not an option for NEC PC98xx computers.) ■ Write To Hard Disk Boot Records: Very few programs write to hard disk boot records. If this activity is detected, it could indicate an unknown virus at work. ■ Write To Floppy Disk Boot Records: Only a few programs (such as the operating system Format command) write to floppy disk boot records. If this activity is detected, it could indicate an unknown virus at work.
Remove alert dialog after ___ seconds	Closes the alert dialog box after it has been displayed for the specified number of seconds.

Setting Lotus Notes and Microsoft Exchange realtime protection advanced options

You can set advanced options for Lotus Notes and Microsoft Exchange realtime scans.

Table 1-4 Lotus Notes and Microsoft Exchange realtime protection advanced options

Option	Description
Scan files inside compressed files	Infected files can be stored inside compressed files. Check to let the antivirus program scan files within compressed files.
Expand ___ levels deep	Specify how many levels deep you want compressed files to be scanned. The contents of compressed files will be scanned with on-demand, scheduled custom, and startup scans. File system realtime protection scans files as they are extracted from compressed files.

Setting Quarantine options

You can set options that determine how managed antivirus clients and servers can forward virus samples to the Quarantine server.

Table 1-5 Quarantine options

Option	Description
Enable Quarantine or Scan And Deliver	Enable this option to use Quarantine or Scan and Deliver.
Allow Forwarding To Quarantine Server	Enable this option to have quarantined files forwarded to the Quarantine server. When this option is selected, clients cannot directly submit items to Symantec Security Response (formerly SARC) from the Quarantine on the client.
Server Name	Enter the server name, IP address, or SPX address of the Quarantine server. (For SPX addresses, use a . [dot] instead of a: [colon] in the SPX address.)
Port	Set the port on which to communicate with the Quarantine server.
Retry	Set the retry interval. The default value is 600 seconds.
Protocol	Select the protocol with which to communicate with the Quarantine server.

Table 1-5 Quarantine options

Option	Description
Allow submissions via Scan and Deliver	Select this option so that clients submit files directly to Symantec Security Response (formerly SARC), and not to the Quarantine server.
Allow files to be resubmitted to SARC	If this option is enabled, files can be submitted to Symantec Security Response (formerly known as SARC) multiple times.
When new virus definitions arrive	Select the action you want Norton AntiVirus to take when new virus definitions arrive.
Quarantine Purge Options	Click to set options that schedule periodic file purging. ■ Enable automatic file purging: Check to enable automatic file purging to occur. ■ Purge After: Purges files after the specified time period; for example, 90 days.
Repaired Items Purge Options	Specify how you want repaired items to be purged. ■ Enable automatic file purging: Check to enable automatic file purging to occur. ■ Purge After: Purges files after the specified time period; for example, 90 days.
Backup Items Purge Options	Specify how you want repaired items to be backed up. ■ Enable automatic file purging: Check to enable automatic file purging to occur. ■ Purge After: Purges files after the specified time period; for example, 90 days.

Setting up clients to receive updates

You can set up clients to receive virus definitions file updates using the following update methods:

- Virus Definition Transport Method
- LiveUpdate

Setting up clients with the Virus Definition Transport Method

With the Virus Definition Transport Method, a push operation starts when new virus definitions are received via the Symantec FTP site or LiveUpdate server by a

primary server on your network. The primary server passes a virus definitions package to all secondary servers in the server group. Secondary servers extract the definitions and place them in the appropriate directory. Clients receive the package from their parent server. Clients extract the definitions and place them in the appropriate directory.

Table 1-6 Virus Definition Manager options for the Virus Definition Transport Method

Option	Description
Update virus definitions from parent server (for managed clients)	Each client retrieves its virus definitions from its parent server.
Check-in Interval	The number of minutes between times when the client checks in with its parent server.

Setting up clients with LiveUpdate

With LiveUpdate, a scheduled and periodic pull operation starts when a client or server on which LiveUpdate is being used requests new definitions. LiveUpdate may be configured on each computer to request the update from a designated internal LiveUpdate server or directly from the Symantec LiveUpdate server.

Table 1-7 Virus Definition Manager options for LiveUpdate

Option	Description
Update virus definitions from parent server	Each client retrieves its virus definitions from its parent server.
Check-in Interval	The number of minutes between times when the client checks in with its parent server.
Schedule Client For Automatic Updates Using LiveUpdate	Use LiveUpdate to perform scheduled updates of the clients. If this option is not selected, the Virus Definition Transport Method is used to update virus definitions.
Frequency	Select the frequency, day, and time that you want the update to occur.
Do not allow client to modify LiveUpdate schedule	Prevents clients from changing the LiveUpdate schedule set from the server. (This option is available when Schedule Client For Automatic Updates Using LiveUpdate is enabled.)

Table 1-7 Virus Definition Manager options for LiveUpdate

Option	Description
Do not allow client to manually launch LiveUpdate	Prevents clients from running LiveUpdate at other than the scheduled times.
Enable continuous LiveUpdate	If a managed Symantec AntiVirus Corporate Edition client infrequently connects to its parent server (for example, a laptop computer that is used offsite), it may not receive the most current virus definitions files updates. For these computers, Continuous LiveUpdate offers a backup option for receiving updates directly from Symantec whenever the computer connects to the Internet.
Download product updates using LiveUpdate	Allows LiveUpdate to update the Norton AntiVirus program on client computers. (This option is available when Schedule Client For Automatic Updates using LiveUpdate is enabled.)

Note: If LiveUpdate is configured to connect to a UNC share on an internal server, the system account must have full rights to network resources. If LiveUpdate is configured to download updates from a UNC share, then LiveUpdate will fail. The system account has no network credentials and must connect to other resources using a null session.

Setting advanced options

You can set options that determine the following:

- How missed events are handled.
- How you want updates to be randomized. (If you are updating many computers at the same time, randomization can decrease server load significantly.)

Table 1-8 Advanced options

Option	Description
Handle missed events within	This option is for events scheduled daily. the antivirus program retries missed scheduled events. It tries to run the scheduled event for the number of hours that you specify.
Perform update within plus or minus	This option is for scheduling virus definitions updates. The event runs at a random time within the number of minutes that you specify.

Table 1-8 Advanced options

Option	Description
Randomize the day of week within	This option is for scheduling virus definitions updates. If this option is selected, the day on which the event runs is chosen at random within the beginning and ending days that you specify.
Randomize the day of the month within plus or minus	This option is available for scheduling virus definitions updates. If this option is selected, the event runs on a random date within the number of days that you specify.

Setting up scheduled scans

Scheduled scans are ideal for scanning large areas of the network. For example, after you download the latest definitions file, you may want to scan all files with it. It is a good idea to schedule scans during off hours when network traffic is low.

Scheduled Scans dialog box

The Scheduled Scans dialog box lets you create new scheduled scans, and edit or delete existing scheduled scans.

Table 1-9 Scheduled Scans dialog box

Option	Description
New	Opens the Scheduled Scan dialog box where you create the schedule (the frequency and time of day) for a new scan.
Edit	Opens the Scheduled Scan dialog box where you can change the frequency and time of day for running a scan.
Delete	Select a scan and click Delete to remove the scan from the schedule.

Scheduled Scan Options dialog box

Name and schedule scans using this dialog box.

Table 1-10 Scheduled Scan Options dialog box

Option	Description
Name	The name assigned to the scheduled scan.

Table 1-10 Scheduled Scan Options dialog box

Option	Description
Scan Settings	Opens the Select Items dialog box where you select the folder to which the settings for this scheduled scan apply.
Enable scan	Allows the scheduled scan to proceed.
Advanced	Opens the Advanced Schedule Options dialog box where you reschedule events that are missed. For example, an event may be missed if a computer is turned off at the time that a scan is scheduled to run.
Frequency	Select how often you want definitions to be updated: daily, weekly or monthly.
At	Specify the time at which you want the updates to occur.

Advanced Schedule Options dialog box

Set advanced scheduling options with this dialog box.

Table 1-11 Advanced Schedule Options dialog box

Option	Description
Handle Missed Events Within	Check to enable a setting that defines how missed events are handled. Missed events includes scans that were scheduled to run when the computer was shut down.
Hours of the Scheduled Time	Set the time limit within which you want the scan to run. For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.

Scan Options dialog box

In the Scan Options dialog box, you can set options that determine how scans run and what actions are taken when a virus is found.

Table 1-12 Scan options dialog box

Option	Description
All Types	Click to scan all files.
Selected Extensions	Click to select the file type extensions that you want to include in the scan.

Table 1-12 Scan options dialog box

Option	Description
Selected Types	Click to select the file types you want to include in the scan. This option is for Windows 3.1x clients.
Macro Virus and Non-Macro Virus Tabs	
Action	Select the action to take when a macro virus is encountered.
If action fails	Select the action to take if the primary action fails when a macro virus is encountered.
Clean virus from file	The antivirus program attempts to clean an infected file as soon as a virus is detected. This is the default setting.
Quarantine infected file	The antivirus program attempts to move the infected file to Quarantine on the infected computer as soon as a virus is detected. After an infected file is moved to Quarantine, you cannot execute it until you take an action (for example, clean or delete) and move the file back to its original location.
Delete infected file	The antivirus program attempts to delete the file. Use this option only if you can replace the infected file with a virus-free backup copy because the file is permanently deleted and cannot be recovered from the Recycle Bin.
Leave alone (log only)	The antivirus program notifies you of the virus and logs the event but does not perform any other action. If you prefer to control how a virus is handled, click the Leave alone (log only) option. When you are notified of the virus, right-click the file name in Virus History, and click one of the following actions: Clean, Delete Permanently, or Move To Quarantine.
Advanced	Opens the Scan Advanced Options dialog box where you can specify in greater detail how a scan is executed.
Display message on infected computer	When the antivirus program detects a virus, you can notify the user of the problem by displaying a warning message on the infected computer's screen.

Table 1-12 Scan options dialog box

Option	Description
Message	Opens the Display Message dialog box where you can create a message. The default message uses message parameters to display pertinent information about the infection on your computer. When displayed on a computer, the message might look like this: Scan type: Scheduled Scan Event: Virus Found Stoned-C File: C:\AUTOEXEC.BAT Location: C: Computer: JSMITH-2 User: JSmith Action taken: Cleaned You can change this message by entering new text or adding message parameters—information placeholders containing changing data.
Exclude files and folders	When checked, the files that you want to exclude from scanning, using file type extensions as the criterion, are excluded from scans.
Exclusions	Opens the Exclusions dialog box where you can specify whether to check the file for exclusion before it is scanned. You can also specify extensions and folders to exclude.
Priority when idle	For scheduled and manual scans, you can control the scan's CPU priority. Giving a scan a lower priority means that the scan will take longer to complete, but also frees the CPU to work on other tasks. You may want to set lower a priority in some situations. For example, if you have scans running at lunch time during the work week, you might want to lower the scan priority to minimize the impact on user productivity. The antivirus server program can throttle its load on NetWare servers. A lower load setting means that the server scan will take longer to complete.
Priority when not idle	A lower load setting means that the server scan will take longer to complete.
Throttle NetWare Load	Check to allow the antivirus server program to throttle its load on NetWare servers based on server load.

Scan Advanced Options dialog box

You can set compressed scan options, remote scanning options, or server scan options from the Scan Advanced Options dialog box.

Table 1-13 Scan Advanced Options dialog box

Option	Description
Scan files inside compressed files	Lets you specify how many levels deep you want compressed files to be scanned. The contents of compressed files are scanned with on-demand, scheduled custom, and startup scans. File system realtime protection scans files as they are extracted from compressed files.
Expand __ levels deep	If you select this option, the antivirus program scans the file archive (such as Files.zip) as well as the individual files of the archive. If the archive contains compressed files, you can specify how many levels deep you want compressed files to be scanned. The default scan setting is three levels deep in a compressed file.
Back up before attempting repair	As a data safety precaution, the antivirus program makes a backup copy of a file before attempting to repair it by default. The backup copy is stored in the Quarantine directory. (The antivirus server for NetWare does not support this option.)
Show scan progress on computer being scanned	When enabled, displays a scan progress window on client computers as they are scanned (during an administrator-initiated manual or scheduled scan).
Close scan progress when done	Closes the scan progress window when a scheduled scan completes. This option is especially useful for unattended computers.
Allow user to stop scan	Displays a Stop button on the scan progress window that provides a user with the ability to cancel a scan in progress.
Storage migration options	Symantec AntiVirus Corporate Edition includes settings that allow you to fine tune scans of files that are maintained by Hierarchical Storage Management (HSM) and offline backup systems. An HSM system migrates files to secondary storage such as CD-ROM, tape jukebox, SAN storage, and so on, but it may leave parts of the original file on the disk. Performance and disk space issues arise during scans if Symantec AntiVirus Corporate Edition opens all of the stubs and the HSM system places the files back on the original disk. Consult your HSM or backup vendor to select the appropriate settings. The settings are dependent on how your HSM application operates.

Table 1-13 Scan Advanced Options dialog box

Option	Description
Skip offline files	If the offline bit is set, the file is skipped. A small clock over a file's icon in Windows Explorer indicates that the offline bit is set. Any application may set the offline bit without actually placing the file offline.
Skip offline and sparse files	Some applications set the file sparse bit to indicate that part of the file is not present on the disk. Because some HSM products set this bit and others don't, consult your HSM vendor to verify whether the sparse bit is set. With a sparse file, a stub of the file remains on the disk with the majority of the file moved to offline storage.
Skip offline and sparse files with a reparse point	Some vendors use reparse points. An application that uses reparse points will also use an appropriate device driver to manage reparse points in the files. This is the default antivirus program setting because it is the most reliable for vendors that use reparse points. Consult your HSM vendor to determine if this setting is appropriate. With a reparse point, a portion of the file remains on disk with the remainder transparently accessed through an application filter (the device driver).
Scan resident portions of offline and sparse files	Symantec AntiVirus Corporate Edition identifies resident portions of a file. If the file is sparse, only the resident portion is scanned; the nonresident portion remains in secondary storage. Because some vendors support this capability and others do not, consult your HSM vendor to determine if this setting is appropriate.
Scan all files, forcing demigration (fills drive)	The entire file is scanned, which forces demigration from secondary storage if necessary. Because the size of the secondary storage is usually greater than the size of the local volume, this setting may fill the local volume and cause further files that are opened for scanning to fail.

Table 1-13 Scan Advanced Options dialog box

Option	Description
Scan all files without forcing demigration (slow)	Symantec AntiVirus Corporate Edition copies a file from secondary storage to the local hard drive as a temp file for scanning, but the HSM application leaves the original file on the secondary storage. This method is slow and not supported by all HSM vendors. Because a file is copied from secondary storage to a disk for scanning, resource demand is high. Processor and network performance may further degrade as infected content is detected when a repair or deletion is returned to secondary storage.
Scan all files recently touched without forcing demigration	To reduce some of the resource demand issues with the Scan all files without forcing demigration option, this option lets you specify that only files that have been migrated recently and may still reside on faster secondary storage are scanned. It may be appropriate to scan files if they still reside on the faster secondary disk, and skip demigration and scanning if the files reside on the slow, long-term storage. For example, files may first be migrated to a remote disk after 30 days of no access. After 60 days of no access, the file is migrated to CD-ROM or remote SAN storage. In many cases, this method may still be slow because accessing files without forcing demigration is a relatively slow operation.
Open files using backup semantics	Allow scanning of files that, for security reasons, are normally not readable except by a specific user.
Scan NetWare compressed or migrated files	Enables scans of files that use NetWare compression and migrated files.

Configuring history deletion

You can determine the frequency with which Virus History, Scan History, and the Event Log data is deleted.

Table 1-14 History option

Option	Description
Delete After	Specify the number and the interval (Days, Months, Years).

Configure LiveUpdate properties

You can configure the Grc.dat to point the client to either of the following:

- Symantec LiveUpdate server
- Internal LiveUpdate server

Setting Symantec LiveUpdate server options

If you have set up a Symantec LiveUpdate server, you can set the option to point computers to it.

Table 1-15 Symantec LiveUpdate Server options

Option	Description
Symantec LiveUpdate Server	Select for the Symantec LiveUpdate Server to serve as the update source.

If you set up an internal LiveUpdate server, you can set options to point computers to it.

Table 1-16 Internal LiveUpdate server options

Option	Description
Name	The name of the server. This name will appear when you run LiveUpdate.
Location	Completing this text box is optional. You can enter descriptive information related to the server. For example, the name of the site.
Login Name	The login name associated with the server. Leave this text box blank so that users can log on and retrieve the files without entering information.
Login Password	The login password associated with the server. Leave this text box blank so that users can log on and retrieve the files without entering information.

Table 1-16 Internal LiveUpdate server options

Option	Description
URL or IP Address	If you are using the FTP method (recommended), select FTP in Type and enter the FTP address for the server. For example: ftp.myliveupdateserver.com. If you are using the HTTP method, select HTTP in Type and enter the Universal Resource Locator for the server. Examples: http:\\myliveupdateserver.com or 155.66.133.11\Export\Home\Ludepot If you are using the LAN method, select LAN in Type and enter the server UNC path name. For example: \\Myserver\LUDepot. In the Login field, enter the name and password to access the server. Specify the Subnet or Subnet mask.
Store passwords in encrypted form	Check for passwords to be encrypted. Encrypted passwords are more secure than unencrypted passwords.

When you leave the Login Name and Login Password text boxes empty, an anonymous logon will be used. This requires that anonymous logons be enabled on the FTP server. If your policy prohibits anonymous logons on FTP servers, enter the logon and password for the FTP server and directory that will be accessed.

Setting client roaming options

You can set options that determine how roaming clients are managed.

Table 1-17 Roaming client support options

Option	Description
Enable Roaming	Check to enable roaming client support.
Validate current parent every ___ minutes	Type the number of minutes between times when the client should check for the availability of its assigned server.
Search for a new (nearest) parent ___ minutes	Type the number of minutes between times that the client should validate that its current parent server is the best choice based on speed and proximity.
Number of samples to average	Number of times that the server will send out packets to help determine the best parent server.
When no new parent is found, wait ____ seconds, then retry	Type the number of minutes between times that the client should retry to validate that its current parent server is the best choice based on speed and proximity.

Table 1-17 Roaming client support options

Option	Description
Server List	You can specify servers for roaming, failover management, and load balancing. ■ Roaming: Click Roaming, then specify the roaming servers. ■ Failover: You can specify backup servers to handle clients when roaming servers are unavailable. A roaming client checks the response time for the first server in the list that answers. If the first backup server goes down, the roaming clients that it manages migrate to the next available backup server in the list when they check their parent server availability. Backup servers do not load balance. Click Failover, then specify the backup servers. ■ Loadbalance: If you have multiple servers and want to distribute roaming clients among them, you can load balance by having roaming servers be treated as equals regardless of how long it takes clients to contact them. A roaming client will contact each server in the list. Roaming servers keep a count of the antivirus programs that they manage, and return this value to the roaming client. The roaming client selects the server with the fewest clients. This server becomes the roaming client's new parent server. Load balancing has a higher priority than finding the closest parent. Click Loadbalance, then specify the names of servers to use in load balancing. ■ Server 1 ■ Server 2

Setting client event forwarding options

You can specify the events that are forwarded to the client's parent server. To choose events to be forwarded, click the Client Event Forwarding button. In the Client Event Forwarding dialog box, select each event that you want to be sent to the parent server. Items that appear grey are automatically forwarded.

Setting immediate manual scan options

You can configure options for a manual scan that will run immediately after the client processes the configurations file.

Table 1-18 Immediate Manual Scan Options dialog box

Options	Description
Configure clients to run a manual scan on grc.dat file processing	Click for a scan to run immediately after the client processes the Grc.dat.
Settings	Launches the Scan Options dialog box. See "Scan Options dialog box" on page 17.

Setting miscellaneous options

You can configure several miscellaneous options for legacy versions of Symantec Anti Virus Corporate Edition 8.0.

Table 1-19 Miscellaneous options

Option	Description
Norton AntiVirus Corporate Edition 7.5	
Enable AMS log forwarding on unmanaged clients	Applies to unmanaged Norton AntiVirus Corporate Edition 7.5 or later clients.
AMS Server Name	Name of the designated AMS server.
Disable the undo action from "on demand" scanning and virus histories	Prevents users from selecting the Undo option for files that may have been quarantined during a scan.

Table 1-19 Miscellaneous options

Option	Description
Number of vdb files kept by client (NT/2000 only)	Applies to managed Windows NT/2000 clients that get virus definitions from antivirus servers. Definitions are updated by virus definitions files that are packaged into a .vdb file. By default, the client stores up to five .vdb files before it begins deleting them. Files are deleted based on their age, with the oldest being deleted first. Changing this value can affect the performance of virus definitions rollbacks since clients will rerequest the old .vdb file from the parent if they do not have the file cached.
Info	Displays detailed information about each of the miscellaneous options.