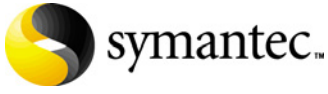
Symantec AntiVirus™ for Linux® Implementation Guide



Symantec AntiVirus™ for Linux® Implementation Guide

Documentation version 1.0

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
http://www.symantec.com

Technical support

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

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

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

www.symantec.com/techsupp/ent/enterprise.html

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you use.

Contacting Technical Support

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

www.symantec.com/techsupp/ent/enterprise.html

Select your region or language under Global Support.

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

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

- Product release level
- Hardware information
- Available memory, disk space, NIC information

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

Licensing and registration

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

www.symantec.com/techsupp/ent/enterprise.html

Select your region or language under Global Support, and then select the Licensing and Registration page.

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/ent/enterprise.html

Select your country or language under Global Support.

- Customer Service is available to assist with the following types of issues:
- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade insurance and maintenance contracts
- Information about Symantec Value License Program
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

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

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

- North America and Latin America: supportsolutions@symantec.com

Additional enterprise services

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

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

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

www.symantec.com

Select your country or language from the site index.

SYMANTEC SOFTWARE LICENSE AGREEMENT
Symantec AntiVirus

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the total number of copies You may use, in any combination of Software titles, may not exceed the total number of copies indicated in the License Module. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. use the Software in accordance with any written agreement between You and Symantec; and
E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antispam software utilize updated antispam rules; antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; policy compliance software utilize updated policy compliance updates; and vulnerability assessment products utilize updated vulnerability signatures; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring

purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of thirty (30) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE**.** The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

A. If the Software You have licensed is a specified Symantec AntiVirus for a corresponding third party product or platform, You may only use that specified Software with the corresponding product or platform. You may not allow any computer to access the Software other than a computer using the specified product or platform. In the event that You wish to use the Software with a certain product or platform for which there is no specified Software, You may use Symantec AntiVirus Scan Engine.

B. If the Software you have licensed is Symantec AntiVirus utilizing Web Server optional licensing as set forth in the License Module, the following additional use(s) and restriction(s) apply:

i) You may use the Software only with files that are received from third parties through a web server;

ii) You may use the Software only with files received from less than 10,000 unique third parties per month; and

iii) You may not charge or assess a fee for use of the Software for Your internal business.

Contents

Technical support

Chapter 1 Introducing Symantec AntiVirus for Linux

About Symantec AntiVirus for Linux 15
About using this guide effectively 16
System requirements 16

Chapter 2 Installing Symantec AntiVirus for Linux

About installing Symantec AntiVirus for Linux 19
    Installation scenarios for Symantec AntiVirus for Linux 20
Installing Symantec AntiVirus for Linux locally 22
Installing Symantec AntiVirus for Linux from a remote server 23
Uninstalling Symantec AntiVirus for Linux 23
    Listing all Symantec AntiVirus packages 23
    About removing Symantec AntiVirus completely 24

Chapter 3 Using Symantec AntiVirus for Linux

When to use the command-line interfaces, services, and tools 25
About the sav command-line interface 28
    About the sav command-line syntax 28
Using the sav CLI to interact with Symantec AntiVirus 33
    Enabling and disabling Auto-Protect 33
    Using Java LiveUpdate 33
    Starting and stopping manual scans 34
    Creating and managing scheduled scans 36
    Managing the local Quarantine 38
    Managing virus definitions 39
    Displaying product information 39
About the symcfg command-line interface 40
    Command-line syntax 40
Using the symcfg CLI to interact with the Symantec AntiVirus configuration database 42
    Listing the keys in the database 42
    Adding a key to the database 42
    Deleting a key from the database 43

About the symcfgd service 43
symcfgd service configuration parameters 43
About the symcfgd files 45
Using the symcfgd service parameters 45
Verifying that the symcfgd service is running 46
Stopping the symcfgd service 46
Starting the symcfgd service 46
Specifying the log facility to use and filtering log messages based on severity 46
About customizing symcfgd 47
About the rtvscand service 47
About the rtvscand service configuration parameters 47
About the rtvscand files 49
Using the rtvscand service parameters 49
Verifying that the rtvscand service is running 50
Stopping the rtvscand service 50
Starting the rtvscand service 50
Specifying the log facility to use and filtering log messages based on severity 51
About customizing the rtvscand service 51
About the savtray program 52
About command-line syntax 52
About savtray parameters 52
About event notification 53

Chapter 4 Updating virus definitions on Linux

About updating virus definitions on Linux 55
About the LiveUpdate Administration Utility 56
About LuAdmin files 57
About Java LiveUpdate 57
About the Java LiveUpdate configuration file 58
Sample liveupdate.conf file 60
About configuring proxy settings in Java LiveUpdate 61
Configuring Java LiveUpdate to use a Central LiveUpdate server 61
Wrapping a liveupdate.conf file in an RPM package 62
Enabling Java LiveUpdate logging on Linux servers 63
Configuring startup options 64
Updating definitions by using Intelligent Updater 67
Downloading and running the script 67
About updating computers individually 68

Chapter 5 Configuring Symantec AntiVirus for Linux

About configuring clients globally by using a GRC.DAT file 69
Configuration by using the Symantec System Center 70
Configuration by using the Configuration Editor tool 70
What you can configure on Linux by using a GRC.DAT file 70
About file exclusions 75
Using the Configuration Editor tool 76
Creating a configuration file 77
Loading and modifying an existing configuration file 78
Saving a configuration file 78
Returning settings to their default configuration 78
Deploying GRC.DAT files 79
Copying a GRC.DAT file 79
Wrapping a GRC.DAT file in an RPM package 79

Index

Chapter 1

Introducing Symantec AntiVirus for Linux

This chapter includes the following topics:

- About Symantec AntiVirus for Linux
- About using this guide effectively
- System requirements

About Symantec AntiVirus for Linux

Symantec AntiVirus™ for Linux® includes real-time antivirus file protection through Auto-Protect scanning, and file system scanning via manual and scheduled scans. You can schedule periodic definitions file updates by using the sav command-line interface or by using the LiveUpdate™ Administration Utility and having your client computers retrieve the updates from a local server.

Note: Scanning for security risks is not enabled by default in Symantec AntiVirus for Linux, but may be enabled by using the GRC.DAT file. If enabled, security risks can be detected and logged, but Symantec AntiVirus cannot take any actions on them.

See "What you can configure on Linux by using a GRC.DAT file" on page 70.

Symantec AntiVirus supports Linux client distribution with RPM Package Manager (RPM) tools and configuration updates with GRC.DAT files.

On Linux distributions, Auto-Protect protects files that are located on the following types of media:

- Hard drives

- Removable media, such as CD ROM drives
- Network file servers

All events that are generated are logged to the standard system log via syslog.

About using this guide effectively

To to use this guide effectively, you should already understand the following:

- The basics of how to administer Linux computers, including tasks such as setting your PATH and environment variables.
- How to use the RPM Package Manager application.
- How to download and install the Java™ Runtime Environment (JRE) on your computers, if it is not already installed.
- If you want to use the client user interface, how to download and install X11, as well as a KDE™ or Gnome™ desktop environment, if this software is not already installed.

System requirements

Symantec AntiVirus requires specific kernels, software, and hardware to run on the Linux operating system.

All requirements for Symantec AntiVirus components are designed to work with the hardware and software recommendations for the supported computers. All Linux computers on which you are installing Symantec AntiVirus should meet or exceed the recommended system requirements for the operating system.

Hardware system requirements

Symantec AntiVirus for Linux requires the following hardware capabilities:

- Intel™ Pentium™ II 266 MHz or higher processor
- 256 MB RAM or higher
- 80 MB free disk space

Software system requirements

Symantec AntiVirus supports the following Linux distributions:

- Red Hat® Enterprise Linux 3.0 ES (RHEL3ES)
- SuSE™ LINUX Enterprise Server 9 (SLES9)
- Novell® Linux Desktop 9 (NLD9)

These distributions are supported on computers using Intel 486-, 586-, and 686-compatible CPUs.

Warning: Auto-Protect functionality is available only on supported kernels. Refer to the Readme file that accompanied your Symantec AntiVirus for Linux software for a list of the supported kernels.

The Java Runtime Environment (JRE) 1.4 or higher must be installed on your Linux computers to use the user interface. JRE is also required to run Java LiveUpdate.

X11 with a KDE or Gnome desktop environment is required to see the system tray icon, user status window, and event notifications.

Chapter 2

Installing Symantec AntiVirus for Linux

This chapter includes the following topics:

- About installing Symantec AntiVirus for Linux
- Installing Symantec AntiVirus for Linux locally
- Installing Symantec AntiVirus for Linux from a remote server
- Uninstalling Symantec AntiVirus for Linux

About installing Symantec AntiVirus for Linux

Symantec AntiVirus uses the RPM Package Manager format for installation. Symantec AntiVirus consists of several installation files, which use the following name format:

<package name>-<major version>.<minor version>.<crt release>-<build number>.<architecture>.rpm

For example, a typical file name might be sav-1.0.0-94.i386.rpm.

Table 2-1 describes the installation packages that are provided.

Table 2-1 Symantec AntiVirus for Linux installation packages

Package	Dependencies	Description
sav	None	The main Symantec AntiVirus program, which implements basic scanning capabilities. Mandatory.

Table 2-1 Symantec AntiVirus for Linux installation packages

Package	Dependencies	Description
savap	kernel version	Symantec AntiVirus Auto-Protect features. Optional. Only specific kernel versions are supported. Refer to the Readme file that accompanied your Symantec AntiVirus for Linux software for a list of the supported kernel versions. **Note:** If you are using an unsupported kernel version, Auto-Protect will not function. However, if you install the savap package on a computer and then later load a supported kernel, Auto-Protect will function.
savui	sav X11 JRE 1.4 or later	The Symantec AntiVirus graphical user interface. X11 must already be installed. Optional.
savjlu	sav JRE 1.4 or later	The Java LiveUpdate features. If this package is not installed, alternative methods must be used to update definitions. Optional. See "About updating virus definitions on Linux" on page 55.

Installation scenarios for Symantec AntiVirus for Linux

Based on your company's environment and needs, you may not want to install all Symantec AntiVirus Linux packages. This section describes some typical installation scenarios.

Note: Refer to the Readme file that accompanied your Symantec AntiVirus software for Linux for a list of the supported kernels.

You have a supported distribution and a supported kernel version

You can install all files and use all the Symantec AntiVirus features, including manual and scheduled scanning, Auto-Protect, the X11-based graphical user interface, and Java LiveUpdate. To do this, your Linux computers must be using supported Linux distributions and supported kernel versions, and have X11 and JRE 1.4 or later installed.

The files can be installed in any order, as long as sav is installed before savui. If you install all files at once, the files are automatically installed in the appropriate order.

You have a supported distribution, but an unsupported kernel version

If you use a supported Linux distribution but use it with an unsupported kernel version, Auto-Protect functionality is not available. You can still use the Symantec AntiVirus manual and scheduled scanning capabilities and Java LiveUpdate to protect the computer.

Note: If you are using an unsupported kernel version, Auto-Protect will not function. However, if you install the savap package on a computer and then later load a supported kernel, Auto-Protect will function.

You should install the following packages:

- sav
- savui
- savjlu

You have a supported distribution and a supported kernel version, but do not use Java

If you use a supported distribution and a supported kernel version, but you do not run Java, then you cannot use Java LiveUpdate to update definitions. You will have to use an alternative method.

See "About updating virus definitions on Linux" on page 55.

You should install the following packages:

- sav
- savui
- savap

You have a supported distribution and a supported kernel version, but do not use X11

If you use a supported distribution and a supported kernel version, but you do not run X11 in your environment, the Symantec AntiVirus user interface is not available on your Linux computers. You can use the sav command line tool to

update definitions. You can use sav command line tool and the computer's syslog to access status and alert messages.

You should install the following packages:

- sav
- savap
- savjlu

You want to use a minimum amount of computing resources

You are running a supported distribution and want a minimal footprint that provides only manual and scheduled scanning. You can do this whether you are running a supported or an unsupported version of the kernel.

You will need to use the sav command line tool and the computer's syslog to access status and alert messages, and to update definitions without using Java LiveUpdate.

See "About updating virus definitions on Linux" on page 55.

You should install only the base sav package.

Installing Symantec AntiVirus for Linux locally

The installation of Symantec AntiVirus for Linux is silent. If desired, you can use the RPM command-line parameter, -Uhv, to display the current percentage of the installation that is complete. A reboot after installation is not required.

The rpm -U command line argument can be used to perform an initial installation or to update an existing installation of Symantec AntiVirus for Linux. Although you can also use the rpm -i command to install, Symantec™ recommends you use -U. The -i command will result in an error if a previous version of Symantec AntiVirus for Linux is already present.

You can install the packages separately or all at once, using wildcard characters, and they will install in the correct order.

To install each file separately

- On the command line, type the following:

```
rpm -Uhv <file_name>.rpm
```

Installing Symantec AntiVirus for Linux from a remote server

RPM allows packages to be installed for the first time from a remote FTP or HTTP server. To do this, you need to supply the name of the remote server on the command line.

You can install from an HTTP server by replacing FTP in the following examples with HTTP, and replacing the <someserver.com> with an HTTP server instead of an FTP server.

To install Symantec AntiVirus for Linux from a remote server

- On the command line, type the following:

  rpm –i ftp://<someserver.com/someshare/file name>.rpm

  If you need to use login credentials for the remote server, type the following:

  rpm –i ftp://<user name:password@someserver.com/someshare/file name>.rpm

Uninstalling Symantec AntiVirus for Linux

Uninstalling Symantec AntiVirus removes installed files from the computer and unregisters the package from the RPM database. If you attempt to uninstall a package that is not currently installed, Symantec AntiVirus returns a message that a package is not installed, but the uninstallation of the other packages still succeeds.

To uninstall Symantec AntiVirus for Linux

1. If you have all packages installed, on the command line, type the following:

   rpm –e sav savap savui savjlu

2. Restart the computer to remove the Auto-Protect support.

Listing all Symantec AntiVirus packages

If you don't remember the package names or which packages are installed, you can use the rpm -qa command to list the installed Symantec AntiVirus packages.

To list all Symantec AntiVirus packages

- On the command line, type the following:

  rpm –qa | grep sav

About removing Symantec AntiVirus completely

After using the rpm -e command to uninstall Symantec AntiVirus, some directories and files still remain. If you need to completely remove Symantec AntiVirus from a computer, you can delete the following directories:

/var/symantec	alert logs and quarantined files
/opt/Symantec/symantec_antivirus	technical support log files
/etc/symantec	the configuration database

You can also safely delete any empty directories that are located under /opt/Symantec.

The following directories may also remain, but should only be deleted if you are sure that there is no Symantec product on the computer that is currently using LiveUpdate:

- /opt/Symantec/virusdefs
- /opt/Symantec/LiveUpdate

The /etc/Symantec.conf file may also remain, but should only be deleted if you are sure that there are no other Symantec products installed on the computer.

Chapter 3

Using Symantec AntiVirus for Linux

This chapter includes the following topics:

- When to use the command-line interfaces, services, and tools
- About the sav command-line interface
- Using the sav CLI to interact with Symantec AntiVirus
- About the symcfg command-line interface
- Using the symcfg CLI to interact with the Symantec AntiVirus configuration database
- About the symcfgd service
- Using the symcfgd service parameters
- About the rtvscand service
- Using the rtvscand service parameters
- About the savtray program

When to use the command-line interfaces, services, and tools

Symantec AntiVirus provides several command-line interfaces (CLIs), services, and tools for configuring and interacting with Symantec AntiVirus when running on Linux.

Note: You must have root privileges to use most of the Symantec AntiVirus for Linux service and command-line interface commands. The exceptions are the sav liveupdate -u and info -a,-d,-e, -p, and -s commands.

Table 3-1 describes the main command-line interfaces and tools and what they are used for.

Table 3-1 Symantec AntiVirus interfaces, services, and tools

Interface or tool	Function
sav command-line interface	This interface provides the primary method of interacting with the Symantec AntiVirus service. You should use this interface for the following tasks: ■ Enabling and disabling Auto-Protect ■ Starting and scheduling LiveUpdates and viewing the current LiveUpdate schedule ■ Starting and stopping manual scans ■ Creating, deleting, enabling, and disabling scheduled scans ■ Viewing a list of scheduled scans and detailed information about each scan ■ Displaying items and acting on items in the local Quarantine ■ Rolling back to a previous version of virus and security risk definitions ■ Using the latest version of local of virus and security risk definitions ■ Displaying general product information
symcfg command-line interface	This interface provides client applications with access to a computer-specific, local configuration database that is used to store configuration data for Symantec AntiVirus for Linux. **Note:** You should use this interface when you need to access Symantec AntiVirus configuration settings that are not accessible through the sav CLI. You should use this interface for the following tasks: ■ Displaying data in the configuration database ■ Adding data to the configuration database ■ Removing data from the configuration database

Table 3-1 Symantec AntiVirus interfaces, services, and tools

Interface or tool	Function
symcfgd service	This service typically runs as a daemon process. This daemon is not typically run from the command line. It is started automatically by the system initialization scripts. If necessary, you can use the parameters that are associated with this service for the following tasks: ■ Specifying the log facility to use when logging to syslog ■ Filtering events that are logged based on severity ■ Stopping the symcfgd daemon ■ Checking to see if the symcfgd service is currently running ■ Changing the working directory for symcfgd ■ Changing the file that holds the PID of the currently running copy of symcfgd
rtvscand service	This service is the interface to rtvscan, the Symantec AntiVirus service that protects Linux client computers from viruses and other security risks. This daemon is not typically run from the command line. It is started automatically by the system initialization scripts. If necessary, you can use the parameters that are associated with this service for the following tasks: ■ Specifying the log facility to use when logging to syslog ■ Filtering the events that are logged based on severity ■ Stopping the rtvscand daemon ■ Displaying help information ■ Checking to see if the rtvscand service is currently running ■ Changing the working directory for rtvscand ■ Changing the file that holds the PID of the currently running copy of rtvscand
savtray command-line interface	This interface runs the Symantec AntiVirus graphical user interface for Symantec AntiVirus for Linux client computers. You should use this interface for the following tasks: ■ Launching the graphical interface with parameters for session management ■ Launching the graphical interface with parameters for controlling the appearance and graphical behavior of Symantec AntiVirus
Configuration Editor tool	If you do not use the Symantec System Center to manage Symantec products in your environment, you can use this tool to create a GRC.DAT file to configure your Symantec AntiVirus Linux client computers. See "Using the Configuration Editor tool" on page 76.

About the sav command-line interface

Symantec AntiVirus for Linux provides a command-line interface for interacting with sav, the basic Symantec AntiVirus service. You can use the sav command-line interface to perform the following tasks:

- enable and disable Auto-Protect, use LiveUpdate
- start and stop manual scans
- list information about scheduled scans
- create and delete scheduled scans
- enable and disable scheduled scans
- manage the local Quarantine
- manage virus definitions
- display product information

The sav commands that produce output produce it in a format that can be parsed by third-party tools. There is no header information for the columns in this output.

About the sav command-line syntax

The general syntax for the sav command line is as follows:

```
sav [--quiet] command parameter(s)
```

The --quiet parameter is the only global parameter for the sav command line.

sav itself does not take wildcard characters, so any wildcard characters that are used on the sav command line are interpreted by the shell that you are using.

You can perform only one action per command line invocation. For example, you cannot turn on Auto-Protect and initiate a LiveUpdate on the same command line.

By default, sav is located in /opt/Symantec/symantec_antivirus.

Note: You must have root privileges to use all of the sav CLI commands except sav liveupdate -u and sav info -a,-d,-e, -p, and -s.

Table 3-2 describes the commands and parameters that are available in the sav command-line interface.

Table 3-2 sav commands and parameters

Command	Parameters	Description
sav	-q|--quiet	Display only the information that is requested; do not display all available information, including status and error messages. This is the only global parameter. This parameter is particularly useful in scripts where you do not want textual error or status messages to appear when the script runs.
sav autoprotect	-e|--enable	Enable Auto-Protect.
sav autoprotect	-d|--disable	Disable Auto-Protect.
sav liveupdate	-u|--update	Perform a LiveUpdate immediately.
sav liveupdate	-v| --view	Display the current LiveUpdate schedule.
sav liveupdate	-s|--schedule <parameters>	Create a new schedule for an automatic LiveUpdate. The following parameters are used to set the schedule: ■ –f <daily|weekly|monthly>|--frequency <daily|weekly|monthly> Mandatory. Specifies the frequency. ■ -i <HH[:]MM|DDD|D>|--interval <HH[:]MM|DDD|D> Mandatory. Identifies the interval of the schedule. If frequency is daily, the interval must be hh[:]mm, where hh is the hour (00-23) and mm is the minute. If frequency is weekly, DDD must be one of the following: Sun, Mon, Tue, Wed, Thu, Fri, Sat. If frequency is monthly, D is any value between 1 and 31. ■ –t hh[:]mm|--time hh[:]mm where hh is the hour (00-23) and mm is the minute (00-59). If no time is specified, this parameter defaults to midnight of the designated interval. Not used for daily frequency.

Table 3-2 sav commands and parameters

Command	Parameters	Description
sav manualscan	-s|--scan [<path_name>...|-]	Initiate a manual scan of the current directory and all its subdirectories. To specify a file and directory list to be scanned, type a list of files and directories, following each item with Enter and ending the list with CTRL-D. If a directory is specified, all subdirectories of that directory are also scanned. Wildcard characters that are used in file names are expanded by the shell. If you use a hyphen instead of a <path_name> argument, then the list of path names is read from the standard input. This is useful when you want to use the output of some other Linux command that produces a list of file names as input to the sav command. You must use commands that produce a list of files or path names separated by line feeds. By default, the maximum number of items that can be added to a manual scan that is generated from the command line interface is 100. You can use symcfg to change the DWORD value VirusProtect6\MaxInput to increase this limit. To remove the limit entirely, you must set it to 0. See "Using the symcfg CLI to interact with the Symantec AntiVirus configuration database" on page 42. **Note:** Submitting a very long list of items to the manualscan command can negatively impact system performance, so Symantec recommends that you limit lists to a maximum of a few thousand items.
sav manualscan	-t|--stop	Stop a manual scan that is in progress.
sav scheduledscan	-l|--list	List all scheduled scans and their current status, either enabled or disabled.
sav scheduledscan	-n|--info <scan ID>	Display detailed information about a specific scan.
sav scheduledscan	-d|--delete <scan ID>	Delete a specific scheduled scan.
sav scheduledscan	-e|--enable <scan ID>	Enable a specific scheduled scan.
sav scheduledscan	-s|--disable <scan ID>	Disable a specific scheduled scan.

Table 3-2 sav commands and parameters

Command	Parameters	Description
sav scheduledscan	-c|--create <scan ID> <parameters> [<path_name>...|-]	Create a new scan identified by the id, which must be unique. The following parameters are available: ■ –f <daily|weekly|monthly> |--frequency <daily|weekly|monthly> Specifies the frequency. ■ -i <HH[:]MM|DDD|D> |--interval <HH[:]MM|DDD|D> Identifies the interval of the schedule. If frequency is daily, the interval must be hh[:]mm, where hh is the hour (00-23) and mm is the minute. If frequency is weekly, DDD must be one of the following: Sun, Mon, Tue, Wed, Thu, Fri, Sat. If frequency is monthly, D is any value between 1 and 31. ■ –t hh[:]mm|--time hh[:]mm Where hh is the hour (00-23) and mm is the minute (00-59). If no time is specified, this parameter defaults to midnight of the designated interval. Not used for daily frequency. ■ –m|--missedevents Enables or disables missed event processing. If enabled, then the scan will run at a later time if the computer is not on at the scheduled time. 0: disabled and 1: enabled. The default value is 0. To specify a list to be scanned, type a list of files and directories, following each item with Enter and ending the list with CTRL-D. If a directory is specified, all subdirectories of that directory are also scanned. Wildcard characters that are used in file names are expanded by the shell. If you use a hyphen instead of a <path_name> argument, then the list of path names is read from the standard input. This is useful when you want to use the output of some other Linux command that produces a list of file names as input to the sav command. You must use commands that produce a list of files or path names separated by line feeds. By default, the maximum number of items that can be added to a scheduled scan that is generated from the command line interface is 100. You can use symcfg to change the DWORD value VirusProtect6\MaxInput to increase this limit. To remove the limit entirely, you must set it to 0. **Note:** Submitting a very long list of items to the scheduledscan command can negatively impact system performance, so Symantec recommends that you limit lists to a maximum of a few thousand items.

Table 3-2 sav commands and parameters

Command	Parameters	Description
sav quarantine	-l|--list	List all items that are in the local Quarantine.
sav quarantine	-d|--delete <ID>	Delete the quarantined item specified. To get the ID of an item in the Quarantine, list the items that are in the Quarantine.
sav quarantine	-r|--restore <ID>	Restore the quarantined item specified. To get the ID of an item in the Quarantine, list the items that are in the Quarantine.
sav quarantine	-p|--repair <ID>	Attempt to repair the specified quarantine item. To get the ID of an item in the Quarantine, list the items that are in the Quarantine.
sav quarantine	-i|--info <ID>	Provide detailed information about the quarantined item specified. To get the ID of an item in the Quarantine, list the items that are in the Quarantine.
sav definitions	-r|--rollback	Roll the definitions file that is used back to the last known good version.
sav definitions	-u|--usenewest	Signal RTVScan to check for new definitions locally and to use them, if new definitions are available.
sav info	-a|--autoprotect	Display the status of Auto-Protect on the computer.
sav info	-d|--defs	Display the version and date of the current virus definitions in use on the computer.
sav info	-e|--engine	Display the version of the scan engine that is currently on the computer.
sav info	-p|--product	Display the version of the product that is currently on the computer.
sav info	-s|--scanner	Display whether or not a scan is in progress on the computer.
sav info	-t|--threats	Display the list of threats and security risks that the computer is currently protected against. **Note:** A user must have root privileges to use this parameter.

Using the sav CLI to interact with Symantec AntiVirus

You can use the sav CLI to perform the following tasks:

- enable and disable Auto-Protect
- start and schedule LiveUpdates and view the current LiveUpdate schedule
- start and stop manual scans
- create, delete, enable, and disable scheduled scans
- view a list of scheduled scans and detailed information about each scan
- display items and act on items in the local Quarantine
- roll back to a previous version of virus and security risk definitions
- use the latest version of local virus and security risk definitions
- display general product information

Note: You must have root privileges to use all of the sav CLI commands except liveupdate -u and info -a,-d,-e, -p, and -s.

Enabling and disabling Auto-Protect

You can use the sav autoprotect command to enable and disable Auto-Protect on a specific computer.

To enable Auto-Protect

- From the command line, type the following:

```
sav autoprotect --enable
```

To disable Auto-Protect

- From the command line, type the following:

```
sav autoprotect --disable
```

Using Java LiveUpdate

You can use the sav liveupdate command to initiate an update using Java LiveUpdate on a specific computer, to view the computer's current LiveUpdate schedule, and to schedule automatic updates using Java LiveUpdate.

There is no managed process for distributing new definitions to clients from a central computer. However, you can do the following:

- use the Intelligent Updater shell script from http://securityresponse.symantec.com/ to update multiple computers.
  See "Updating definitions by using Intelligent Updater" on page 67.
- use the LiveUpdate Administration Utility to set up a Central LiveUpdate server on your network and configure Java LiveUpdate to point your clients to pick up definitions updates from that server.
  See "About the LiveUpdate Administration Utility" on page 56.
  See "Configuring Java LiveUpdate to use a Central LiveUpdate server" on page 61.

To start an immediate LiveUpdate

- From the command line, type the following:
  ```
  sav liveupdate --update
  ```

To view the current LiveUpdate schedule

- From the command line, type the following:
  ```
  sav liveupdate --view
  ```

To schedule an automatic LiveUpdate

- From the command line, type the following:
  ```
  sav liveupdate --schedule -f <frequency> -i <interval> -t <time>
  ```
  For example, to schedule an automatic LiveUpdate that runs every Friday at 11:30 P.M., type the following:
  ```
  sav liveupdate --schedule -f weekly -i Fri -t 23:30
  ```
  For example, to schedule an automatic LiveUpdate that runs only on the second day of the month at 3 A.M., type the following:
  ```
  sav liveupdate --schedule -f monthly -i 2 -t 3:00
  ```

Starting and stopping manual scans

You can use the sav manualscan command to start and to stop a manual scan on a specific computer.

If you use a hyphen (-) as the <path_names> argument when starting a manual scan, the list of <path_names> is read from the standard input. This is useful if you want to use the output of another Linux command that produces a list of file names as input to sav. Use commands that produce a list with a line feed between each item.

By default, the maximum number of items that can be added to a manual scan that is generated from the command line interface is 100. You can use symcfg to change the DWORD value VirusProtect6\MaxInput to increase this limit. To remove the limit entirely, you must set it to 0.

See "Using the symcfg CLI to interact with the Symantec AntiVirus configuration database" on page 42.

Note: Submitting a very long list of files to the manualscan command can negatively impact system performance, so Symantec recommends that you limit file lists to a maximum of a few thousand items.

To start a manual scan of a directory and its subdirectories

- From the command line, type the following:

  ```
  sav manualscan --scan <path_name>
  ```

  For example, to start a manual scan of user John's directory in the /home directory, type the following:

  ```
  sav manualscan --scan /home/john
  ```

To start a manual scan with input from another command

- From the command line, type the following:

  ```
  <other command> | sav manualscan --scan -
  ```

  Use commands that produce a list of items separated by line feeds. For example, to start scan of all files that have been modified within the last hour in or below a user's home directory, type the following:

  ```
  find ~john -mmin -60 -type f -print | sav manualscan --scan -
  ```

To type a list of files and directories to be scanned

- From the command line, type the following:

  ```
  sav manualscan --scan -
  <file name> ENTER
  <path name> ENTER
  <path name> ENTER
  <filename> CTRL-D
  ```

To stop a manual scan that is in progress

- From the command line, type the following:

  ```
  sav manualscan --stop
  ```

Creating and managing scheduled scans

You can create, enable and disable, list, and display detailed information about a particular scheduled scan from the command line.

By default, the maximum number of items that can be added to a scheduled scan that is generated from the command line interface is 100. You can use symcfg to change the DWORD value VirusProtect6\MaxInput to increase this limit. To remove the limit entirely, you must set it to 0.

Note: Submitting a very long list of files to the scheduledscan command when creating a scheduled scan can negatively impact system performance, so Symantec recommends that you limit lists to a maximum of a few thousand items.

Listing information about scheduled scans

If you list the scheduled scans on a computer, the output looks similar to the following:

```
SS01    Weekly: Mon    Enabled    Done

SS02    Daily: 11:15   Disabled   Never Run

SS03    Monthly: 25    Disabled   Never Run
```

The columns provide the following information:

- Column 1 is the name that was given to the scan when the scan was created; also called the scan ID.
- Column 2 is the frequency and time of the scan.
- Column 3 is the scan status: Enabled or Disabled.
- Column 4 reports the current state of the scan: Running, Done, or Never Run.

To list the scheduled scans on a computer

- From the command line, type the following:

  sav scheduledscan --list

To list detailed information about a particular scan

- From the command line, type the following:

  sav scheduledscan --info <scan ID>

Creating and deleting a scheduled scan

You can use the scheduledscan command to create and delete a scheduled scan on a specific computer.

To create a scheduled scan

- From the command line, type the following:

  sav scheduledscan --create <scan ID> -f <frequency> -i <interval> -t <time> -m <missed event processing value> <path name>...

  For example, suppose you want to create a scheduled scan named myschedscan that scans the /usr directory, runs every Saturday at 11:01 P.M., and will not run when the computer is next turned on, if the computer is not on at the scheduled time. To create this scan, from the command line, type the following:

  sav scheduledscan --create myschedscan -f weekly -i Sat -t 23:01 -m 0 /usr

To create a scheduled scan by using input from another command

- From the command line, type the following:

  <other command> | sav scheduledscan --create <scan ID> -f <frequency> -i <interval> -t <time> -m <missed event processing value> -

  Use commands that produce a list of items separated by line feeds. For example, to schedule a daily scan of all files that have been modified within the last eight hours in or below Steve's home directory, type the following:

  find ~steve -mmin -480 -type f -print | sav scheduledscan --create stevescan -f daily -i 17:01 -m 0 -

To delete a scheduled scan

- From the command line, type the following:

  sav scheduledscan --delete <scan ID>

  where <scan ID> is the name you gave to the scan when you created it.

Enabling and disabling a scheduled scan

You can use the scheduledscan command to enable and disable a scheduled scan.

To enable a scheduled scan

- From the command line, type the following:

  sav scheduledscan --enable <scan ID>

  where <scan ID> is the name you gave to the scan when you created it.

To disable a scheduled scan

- From the command line, type the following:
  sav scheduledscan --disable <scan ID>
  where <scan ID> is the name that you gave to the scan when you created it.

Managing the local Quarantine

You can use the sav quarantine command to do the following:

- list the items in the Quarantine
- display detailed information about an item in the Quarantine on a specific computer
- delete and restore items from the Quarantine
- attempt to repair an item in the Quarantine

To list the files in the local Quarantine

- From the command line, type the following:
  sav quarantine --list

To display detailed information about a file in the local Quarantine

- From the command line, type the following:
  sav quarantine --info <ID>
  where <ID> is the ID of the item. Obtain the ID of a item by listing the items that are in the local Quarantine.

To delete a file in the local Quarantine

- From the command line, type the following:
  sav quarantine --delete <ID>
  where <ID> is the ID of the item. Obtain the ID of a item by listing the items that are in the local Quarantine.

To restore a file in the local Quarantine

- From the command line, type the following:
  sav quarantine --restore <ID>
  where <ID> is the ID of the item. Obtain the ID of a item by listing the items that are in the local Quarantine.

To repair a file in the local Quarantine

- From the command line, type the following:
  sav quarantine --repair <ID>

where <ID> is the ID of the item. Obtain the ID of a item by listing the items that are in the local Quarantine.

Managing virus definitions

You can use the sav definitions command to roll back the virus and security risk definitions to the last known good version or to have the computer check for and use the latest local version of definitions on a specific computer.

To roll back to the last known good version of definitions

- From the command line, type the following:

```
sav definitions --rollback
```

To use the latest local version of definitions

- From the command line, type the following:

```
sav definitions --usenewest
```

Displaying product information

You can use the sav info command to display general product information about a specific computer, including the following:

- the status of Auto-Protect
- the version and date of the current virus definitions
- the product version that is in use
- the version of the scan engine that is in use
- whether or not a scan is in progress
- the list of threats and security risks that the computer is currently protected against

To display the status of Auto-Protect

- From the command line, type the following:

```
sav info --autoprotect
```

To display the virus definitions version

- From the command line, type the following:

```
sav info --defs
```

To display the current product version

- From the command line, type the following:
  sav info --product

To display the current scan engine version

- From the command line, type the following:
  sav info --engine

To determine if a scan is in progress

- From the command line, type the following:
  sav info --scanner

To display the list of threats that the computer is protected from

- From the command line, type the following:
  sav info --threats

About the symcfg command-line interface

symcfg is a command-line tool that provides client applications with access to a computer-specific, local configuration database that is used to store configuration data for Symantec AntiVirus. Configuration settings are stored in a data file in binary format, not as text. The symcfg tool can be used to display, create, remove, and change the value of data that is stored in this database.

Command-line syntax

You cannot use multiple symcfg commands and their parameters as part of the same command line.

You must use the following syntax for the symcfg command lines:

```
symcfg [-q|--quiet] [-r|--recursive]

symcfg [-q|--quiet] [-r|--recursive] add -k|--key key [-v|--value
value -d|--data data -t|--type type]

symcfg [-q|--quiet] [-r|--recursive] delete -k|--key key [-v|--value
value]

symcfg [-q|--quiet] [-r|--recursive] list -k|--key [key|*] [-v|--
value value]
```

Note: You must have root privileges to use symcfg.

By default, symcfg is located in /opt/Symantec/symantec_antivirus.

Note: You may need to enclose key names in single quotes to prevent the backslash from being interpreted as an escape character by the shell.

Table 3-3 describes the commands and parameters that are available for symcfg.

Table 3-3 symcfg commands and parameters

Command	Parameters	Description
symcfg	-q [command] --quiet [command]	Display only the information that is being requested; suppress error messages.
symcfg	-r --recursive	Apply the command that follows recursively.
symcfg add	N/A	Create new keys and values in the database, or overwrite existing ones.
symcfg add	-k key --key key	The name of the key to add or overwrite. Mandatory. **Note:** If no corresponding value is given, only the key is created.
symcfg add	-v value --value value	The name of the value to add or overwrite.
symcfg add	-d data --data data	The data to store for the value/data pair.
symcfg add	-t type --type type	One of the following constants, representing the data type the following: ■ reg_sz (string) ■ reg_dword (32-bit unsigned integer) ■ reg_binary (arbitrary binary data)
symcfg delete	N/A	Remove keys and values from the database.
symcfg delete	-k key --key key	The name of the key to delete. Mandatory. **Note:** If no corresponding value is given, the key and all of its values are deleted. If there are subkeys present, the delete fails.
symcfg delete	-v value --value value	The name of the value to remove.
symcfg list	N/A	List all the values and keys for a given key.

Table 3-3 symcfg commands and parameters

Command	Parameters	Description
symcfg list	-k key --key [key|*]	The name of the key to list. To list all keys from the root node, use an asterisk (*) instead of a key name. Mandatory. If used without the --value parameter, all subkeys and values for this key are listed. **Note:** You must escape an asterisk or enclose it in quotes to protect it from being expanded by the shell.
symcfg list	-v value --value value	The name of the value to list. The value is displayed in the following format: \<key>\<subkey>\<value name> <value data> <value type>. For example: \VirusProtect6\Storages\FileSystem\ServiceStatus 1 REG_DWORD

Using the symcfg CLI to interact with the Symantec AntiVirus configuration database

The symcfg CLI provides access to some configuration settings stored in the local configuration database that are not accessible through the sav CLI.

Note: You must have root privileges to use the symcfg command-line interface.

Listing the keys in the database

You can list all the keys that are stored in the database.

To list the keys in the database

- From the command line, type the following:

  ```
  symcfg list -k <key> [-v <value>]
  ```

  For example, to list all keys under the Storages node, you would type the following:

  ```
  symcfg -r list -k 'VirusProtect6\Storages'
  ```

Adding a key to the database

You can add keys and their corresponding values to the database to configure Symantec AntiVirus.

To add a key to the database

- From the command line, type the following:
  symcfg add -k <key> [-v <value>] [-d <data>] [-t <type>]
  For example, to add a key to the database to exclude the /tmp/no_scan directory from Auto-Protect scans, you would type the following:
  symcfg add --key
  VirusProtect6\Storages\Filesystem\RealTimeScan\NoScanDir
  --value /tmp/no_scan --data 1 --type REG_DWORD

Deleting a key from the database

You can delete keys and their corresponding values from the database to configure Symantec AntiVirus.

To delete a key from the database

- From the command line, type the following:
  symcfg delete -k <key> [-v <value>] [-d <data>] [-t <type>]
  For example, to delete the scan1 from the database, you would type the following:
  symcfg delete -k "VirusProtect6\Custom Tasks\scan1"

About the symcfgd service

symcfgd is the Symantec configuration service, which runs as a daemon process. This service is typically started automatically by the system initialization scripts. No changes to the default values should be required.

Note: This implementation uses a small number of kernel semaphores, which are shared among applications. Although unlikely, it is possible that Auto-Protect could experience problems if the operating system has an insufficient number of semaphores allocated for the computer. If the allocation of a semaphore fails, an event appears in the syslog. If necessary, you can increase the number of semaphores that are allocated for the operating system to alleviate the problem.

---

symcfgd service configuration parameters

The parameters available for interacting with the symcfgd are used by the /etc/sysconfig/symcfgd file, but can also be used from the command line if special handling is required.

Table 3-4 describes the parameters that are available for interacting with the symcfgd service.

Table 3-4 symcfgd service configuration parameters

Parameter	Description
-f <log_facility>	Specifies the log facility to use when logging to syslog. Possible values are as follows: ■ daemon (default) ■ user ■ local0 through local7 To set this up, you must also configure your /etc/syslog.conf file to specify handling for the facility.
-h	Displays help information.
-k shutdown | check	Sends a specified signal to the running copy of symcfgd, and then exits. The running copy is identified as the process that has the pid that matches the pid stored in the pid file. This parameter has the following arguments: ■ Shutdown sends a signal to shut down the running copy. The process attempts to perform a graceful shutdown. ■ Check determines if symcfgd is currently running, and then prints out a message. If there is a running copy, the command returns a 0. If there is no running copy, the command returns a 1. **Note:** When specifying the -k parameter and using a nondefault pid file, the -p parameter must also be given to ensure that the signal is sent to the correct symcfgd instance, even if there is only a single symcfgd instance running.
-l severity	Logs all messages up to and including the specified severity level. Severity must be one of the following: none, emerg, alert, crit, error, warning, notice, info, debug.
-p <absolute_path>	Specifies to use the given process ID (pid) file instead of the default /var/run/symantec/symcfgd.pid file. You should always use absolute path names when configuring symcfgd. By default, /var/run/symantec/symcfgd.pid stores the process ID (pid) of the currently running copy of symcfgd. When symcfgd is terminated, this file is deleted.
-s <absolute_path>	Sets the working directory that the service runs in. You should always use absolute path names when configuring symcfgd. **Note:** This option typically does not need to be changed from the default value, which is the root directory (/).

Note: If you are using a nondefault pid file, you must give the -p parameter when using the -k parameter, to send the signal to the correct symcfgd instance, even if there is only a single instance running.

About the symcfgd files

Table 3-7 describes the files that are used for the symcfgd service.

Table 3-5 Description of the symcfgd service files

File	Description

/etc/sysconfig/symcfgd	This configuration file specifies command-line parameters that are passed to the symcfgd program when it is started with the init.d script. To use this file, you must set the parameters to symcfgd between the quotes in the following line:
	`SYMCFGD_OPTS=""`
	For example, to log to the local0 facility and only log up to the error level of severity, you would use the following:
	`SYMCFGD_OPTS="-f local0 -l error"`

/usr/etc/rc.d/init.d/symcfgd	This file is the symcfgd startup and shutdown script. This script supports the expected init.d commands, such as start, stop, restart, and so on. The chkconfig command is used to enable or disable the automatic startup of the symcfgd daemon.
/var/run/symantec/symcfgd.pid	This file stores the process ID (pid) of the currently running symcfgd. When the currently running symcfgd service is terminated, this file is deleted.

Using the symcfgd service parameters

You can check to see if symcfgd is running, stop symcfgd gracefully, and start it up again.

Note: You must have root privileges to use symcfgd.

You should typically use the /etc/init.d/symcfgd initialization script to perform most tasks that involve the symcfgd service. Using the initialization script

ensures that any parameters you have set are picked up when you interact with the service.

Note: Different Linux distributions may have slightly different paths to the startup script directory, but for interoperability, the path /etc/init.d/ should always resolve to the correct startup script directory.

Verifying that the symcfgd service is running

You can use the /etc/init.d/symcfgd initialization script to verify that the rtvscand service is running. Be sure to specify the absolute path to the script.

To verify that the symcfgd service is running

- From the command line, type the following:
  `/etc/init.d/symcfgd status`

Stopping the symcfgd service

You may want to stop the symcfgd service temporarily. When using the /etc/init.d/symcfgd initialization script, be sure to specify the absolute path to the script.

To stop the symcfgd service

- From the command line, type the following:
  `/etc/init.d/symcfgd stop`

Starting the symcfgd service

When using the /etc/init.d/symcfgd initialization script, be sure to specify the absolute path to the script.

To start the symcfgd service

- From the command line, type the following:
  `/etc/init.d/symcfgd start`

Specifying the log facility to use and filtering log messages based on severity

You can use the symcfgd -f parameter to log messages using any of the general purpose Linux syslog facilities. To set this up, you must also configure your /etc/syslog.conf file to specify handling for the facility.

You can use the following facilities: daemon, user, local0, local1, local2, local3, local4, local5, local6, and local7. The default facility is daemon.

You can use the symcfgd -l parameter with a severity level to filter the messages that are logged. <level> must be one of the following: none, emerg, alert, crit, error, warning, notice, info, or debug.

Messages up to and including the specified severity level are logged. For example, if you specify crit, only the messages that are labelled emergency, alert, and critical are logged.

For more information about how you can use these parameters, you can refer to the logger(1), syslog(3), and syslogd(8) man pages on your Linux computer.

About customizing symcfgd

The symcfgd defaults on Linux should work with no changes in any environment. However, if your environment requires that you use a custom initialization script to accommodate specialized functionality, you can use the service parameters from the command line.

Use the following syntax from the command line:

```
symcfgd [-h] [-f log_facility] [-k shutdown|check] [-l severity]
[-p pid_file] [-s path]
```

You must have root privileges to use the symcfgd command-line interface.

About the rtvscand service

The rtvscand service is the interface to rtvscan. rtvscan is the Symantec AntiVirus service that protects Linux client computers from viruses and other security risks. rtvscand performs scans of the file system at the request of Auto-Protect and users.

This service is typically started automatically by the system initialization scripts. No changes to the default values should be required.

About the rtvscand service configuration parameters

The rtvscand parameters are used by the /etc/sysconfig/rtvscand file, but can also be used from the command line if special handling is required.

Table 3-6 describes the parameters that are available for interacting with the rtvscand service.

Table 3-6 rtvscand service configuration parameters

Parameter	Description
-f <log_facility>	Specifies the log facility to use when logging to syslog. Possible arguments are as follows: ■ daemon (default) ■ user ■ local0 through local7 To set this up, you must also configure your /etc/syslog.conf file to specify handling for the facility.
-h	Displays help information.
-k shutdown | check	Sends a specified signal to the running copy of rtvscand, and then exits. The running copy is identified as the process that has the pid that matches the pid stored in the pid file. This parameter has the following arguments: ■ Shutdown sends a signal to shut down the running copy. The process attempts to perform a graceful shutdown. ■ Check determines if rtvscand is currently running and prints out a message. If there is a running copy, the command returns a 0. If there is no running copy, the command returns a 1. **Note:** When specifying the -k parameter and using a nondefault pid file, the -p parameter must also be given to ensure that the signal is sent to the correct rtvscand instance, even if there is only a single rtvscand instance running.
-l severity	Logs all messages up to and including the specified severity level. Severity must be one of the following: none, emerg, alert, crit, error, warning, notice, info, debug.
-p <absolute_path>	Specifies to use the given process ID (pid) file instead of the default /var/run/symantec/rtvscand.pid file. You should always use absolute path names when configuring rtvscand. By default, /var/run/symantec/rtvscand.pid stores the process ID (pid) of the currently running copy of rtvscand. When rtvscand is terminated, this file is deleted.
-s <absolute_path>	Sets the working directory that the service runs in. You should always use absolute path names when configuring rtvscand. **Note:** This typically does not need to be changed from the default, which is the root directory (/).

Note: If you are using a nondefault pid file, you must give the -p parameter when using the -k parameter, to send the signal to the correct rtvscand instance, even if there is only a single instance running.

About the rtvscand files

Table 3-7 describes the files that are used for the rtvscand service.

Table 3-7 Description of the rtvscan service files

File	Description

/etc/sysconfig/rtvscand	This configuration file specifies command-line parameters that are passed to the rtvscand program when it is started with the init.d script. To use this file, you must set the parameters to rtvscand between the quotes in the following line:
	`RTVSCAND_OPTS=""`
	For example, to log to the local0 facility and only log up to the error level of severity, you would use the following:
	`RTVSCAND_OPTS="-f local0 -l error"`

/usr/etc/rc.d/init.d/rtvscand	This file is the rtvscand startup and shutdown script. This script supports the expected init.d commands, such as start, stop, restart, and so on. The chkconfig command is used to enable or disable the automatic startup of the rtvscand daemon.
/var/run/symantec/rtvscand.pid	This file stores the process ID (pid) of the currently running rtvscand. When the currently running rtvscand service is terminated, this file is deleted.

Using the rtvscand service parameters

You can check to see if rtvscand is running, stop rtvscand gracefully, change its working directory, and change the file that is used to store the PID of the running copy of rtvscand.

Note: You must have root privileges to use rtvscand.

Although you can use the parameters from the command line, you should typically use the /etc/init.d/rtvscand initialization script to perform most tasks that involve the rtvscand service. Using the initialization script ensures that any parameters you have set are picked up when you interact with the service.

Note: Different Linux distributions may have slightly different paths to the startup script directory, but for interoperability, the path /etc/init.d/ should always resolve to the correct startup script directory.

Verifying that the rtvscand service is running

You can use the /etc/init.d/rtvscand initialization script to verify that the rtvscand service is running. Be sure to specify the absolute path to the script.

To verify that the rtvscand service is running

- From the command line, type the following:

```
/etc/init.d/rtvscand status
```

Stopping the rtvscand service

You may want to stop the rtvscand service temporarily. If you do, you should restart rtvscand as soon as possible to protect the computer, because many risks can go undetected when rtvscand is not running. You can use the /etc/init.d/rtvscand initialization script to stop the rtvscand service. Be sure to specify the absolute path to the script.

To stop the rtvscand service

- From the command line, type the following:

```
/etc/init.d/rtvscand stop
```

Starting the rtvscand service

You can restart rtvscand by running the rtvscand startup script. Be sure to specify the absolute path to the script.

Note: Different Linux distributions may have slightly different paths to the startup script directory, but for interoperability, the path /etc/init.d/ should always resolve to the correct startup script directory.

The symcfgd service must be running for rtvscand to operate. If you are using the default /etc/init.d/rtvscand script to start rtvscand, the script will check to see if symcfgd is running and start symcfgd if it is not currently running.

To start the rtvscand service

- From the command line, type the following:
  `/etc/init.d/rtvscand start`

Specifying the log facility to use and filtering log messages based on severity

You can use the rtvscand -f parameter to log messages using any of the general purpose Linux syslog facilities. To set this up, you must also configure your /etc/syslog.conf file to specify handling for the facility.

You can use the following facilities: daemon, user, local0, local1, local2, local3, local4, local5, local6, and local7. The default is facility daemon.

You can use the rtvscand -l parameter with a severity level to filter the messages that are logged. <level> must be one of the following: none, emerg, alert, crit, error, warning, notice, info, or debug.

Messages up to and including the specified severity level are logged. For example, if you specify crit, only the messages that are labelled emergency, alert, and critical are logged.

For more information about how you can use these parameters, you can refer to the logger(1), syslog(3), and syslogd(8) man pages on your Linux computer.

About customizing the rtvscand service

The rtvscand service default values should work in any Linux environment. However, if your environment requires that you use a custom initialization script to accommodate specialized functionality, you can use the service parameters to make changes from the command line.

Use the following syntax for the rtvscand command line:

```
rtvscand [-h] [-f log_facility] [-k shutdown|check] [-l severity]
[-p pid_file] [-s path]
```

Note: You must have root privileges to use rtvscand.

About the savtray program

The savtray program is a Symantec AntiVirus graphical user interface tool for viewing Symantec AntiVirus status, program, scan engine, and virus and security risk definitions versions; notifying you of risk events; and starting a LiveUpdate session on the computer.

In the KDE and Gnome desktop environments, Symantec AntiVirus for Linux provides a yellow shield icon on the status tray. If Symantec AntiVirus is disabled, the icon appears with a black exclamation point next to the shield; if Auto-Protect is disabled, the shield appears with a red circle and a slash through it.

The user interface allows users to do the following:

- Display status and version information, including the version of the program, scan engine, and virus definitions that are in use.
- View risk information found by Auto-Protect or by a scan, if the user has read permission in the directory where the risk was found. If more than one risk is found, users can page through the information.
- Perform LiveUpdates from the status window, unless you have configured Symantec AntiVirus to not allow users to run LiveUpdate.

About command-line syntax

You can use the following syntax for the savtray command line:

```
savtray [-bg color|-background color] [-btn color|-button color]
[-cmap] [-display display] [-fg color|-foreground color]
[-fn font|-font font] [-geometry geometry] [-name name]
[-ncols count] [-reverse] [-session[=]session] [-style[=]style]
[-title title] [visual TrueColor] [-widgetcount]
```

About savtray parameters

Table 3-8 describes the parameters that are available for managing the savtray user interface.

Table 3-8 savtray parameters

Parameter	Description
-bg <color> -background <color>	Sets the default background color and an application palette. Light and dark shades are calculated.

Table 3-8 savtray parameters

Parameter	Description
-btn <color> -button <color>	Sets the default button color.
-cmap	Causes the application to install a private color map on an 8-bit display.
-display <display>	Specifies the name of the X server to use. The default is $DISPLAY.
-fg <color> -foreground <color>	Sets the default foreground color that is used for text and graphics.
-fn <font> -font <font>	Defines the application font. The font should be specified using an X logical font description.
-geometry <geometry>	Specifies the initial size and location of the window.
-name <name>	Sets the application name.
-ncols <count>	Limits the number of colors that are allocated on an 8-bit display.
-reverse	Causes text to be formatted for right-to-left languages rather than for left-to-right languages.
-session=<session> -session <session>	Restores the application from an earlier session.
-style=<style> -style <style>	Sets the application GUI style. Possible values are motif, windows, and platinum.
-title <title>	Sets the application caption.
-visual TrueColor	Forces the application to use a TrueColor visual on an 8-bit display.
-widgetcount	When the program exits, prints a debug message that states the number of widgets left undestroyed and the maximum number of widgets that existed simultaneously.

About event notification

If a user is using a KDE or Gnome environment with the savtray package installed, they will get notifications of events under some circumstances.

If a user's action, such as opening a file, triggers the detection of a risk, the user will get a notification dialog box from Auto-Protect. On multi-user machines, users will see a notification only if their own action triggered the detection of the risk. Since only users with root privileges can run manual and scheduled scans, most users will never see notifications of risks that are found by these scans.

Users with root privileges will get a notification dialog box if risks are found during a manual scan or scheduled scan while they are logged on. They will also see a notification dialog box when Auto-Protect detects a risk that is triggered by one of their actions.

Note: All generated events are logged to the standard system log via syslog, regardless of which user triggers their detection and whether Symantec AntiVirus detects them via Auto-Protect or a manual or scheduled scan.

Chapter 4

Updating virus definitions on Linux

This chapter includes the following topics:

- About updating virus definitions on Linux
- About the LiveUpdate Administration Utility
- About Java LiveUpdate
- About configuring proxy settings in Java LiveUpdate
- Configuring Java LiveUpdate to use a Central LiveUpdate server
- Enabling Java LiveUpdate logging on Linux servers
- Updating definitions by using Intelligent Updater
- About updating computers individually

About updating virus definitions on Linux

You can update the virus and security risk definitions on your Linux client computers in the following ways:

- Use the LiveUpdate Administration Utility, LuAdmin, to set up a Central LiveUpdate server on your network and configure Java LiveUpdate to point your clients to pick up definitions updates from that server.
- Use an Intelligent Updater shell script.
- Initiate a manual LiveUpdate from the user interface or command line on the computer.

Note: The definitions file and Intelligent Updater script that are used for Linux computers are not the same as the definitions file and Intelligent Updater script that are used on Windows® computers.

About the LiveUpdate Administration Utility

The LiveUpdate Administration Utility, luau.exe, is a self-extracting compressed archive that allows you to download update packages and configure clients to retrieve those updates from an internal proxy server. It is used to set up a central LiveUpdate server on your internal network. Rather than all client computers contacting the Symantec servers to obtain definitions and product updates, the client computers contact a Central LiveUpdate server on your local network.

Note: You must install and run LuAdmin on a Windows 2000 Professional/2003/XP Professional 32-bit, SP 2 computer. It is not available for Linux computers.

Using a Central LiveUpdate server means that clients do not need to connect to an external network for virus definitions and product updates. This reduces WAN traffic and transfer speeds and can be used by clients who do not have access to the Internet, but are part of the network. It also allows updating definitions for unmanaged clients and allows you to manage bandwidth usage for definitions updates by scheduling when LiveUpdate runs. In addition, using a Central LiveUpdate server gives you control over the types of updates that are available to users.

You can use LuAdmin to perform the following tasks:

- Select the Symantec products and languages for which updates will be downloaded
- Specify the full path to the directory in which downloads will be stored
- Retrieve all of the update packages and related index files from the Symantec LiveUpdate site that apply to the selected products

LuAdmin is typically installed on one computer on the network. LuAdmin does not need to be installed on the same server that is used as the Central LiveUpdate server. If you set up the Central LiveUpdate server on a separate computer, then you can test new updates before moving them to the Central LiveUpdate server.

Warning: The LuAdmin packages that are downloaded can be large, so Symantec does not recommend this method for networks with slow Internet connections, especially dial-up connections.

About LuAdmin files

The files that you need to install and use LuAdmin are located on the Symantec AntiVirus Win32 CDs in the \Tools\LiveUpdate directory. You will need the following:

- luau.exe, the LuAdmin Utility
- luadmin.pdf, the *LiveUpdate Administrator's Guide*

Note: If you already have the latest version of LuAdmin installed on a computer in your network, you do not need to install the copy that is provided with this product.

For information about installing LuAdmin, setting up a central LiveUpdate server, and downloading updates, refer to the *LiveUpdate Administrator's Guide*.

About Java LiveUpdate

Java LiveUpdate is the Symantec technology that provides LiveUpdate services on Windows server products and non-Win32 operating systems, such as Linux.

Java LiveUpdate functions similarly to the Win32 version of LiveUpdate. When Java LiveUpdate runs, it connects to the server that is specified in the host file or in the liveupdate.conf file.

Java LiveUpdate determines if there are updates available for the specified products. For each update that is found, a temporary directory is created under the local package directory into which the zipped files are copied. The packages are authenticated, unzipped, and installed. The temporary directory and files are then removed.

Java LiveUpdate tracks configuration information about multiple LiveUpdate servers or hosts. It tries each of the servers in the order in which they are listed in the Java LiveUpdate configuration file, and automatically fails over to the next host if it finds that the server is unreachable.

About the Java LiveUpdate configuration file

By default, Java LiveUpdate gets its configuration information from the liveupdate.conf file. The liveupdate.conf file on Linux is located in /etc.

Table 4-1 describes the parameters that you can set when you configure Java LiveUpdate.

Table 4-1 liveupdate.conf file parameters

Parameter	Description
workdir	The working directory on the client computer. This entry is required. Java LiveUpdate creates a local package directory under the specified working directory. If the working directory does not exist, Java LiveUpdate creates it and uses the working directory as the local package directory. The local package directory is removed when Java LiveUpdate exits, unless the -k command-line parameter is specified.
logfile	The full path to the log file that Java LiveUpdate uses to log events and errors. If this setting is omitted, no log file is created.
jar	The full path to the jlu.jar file. If this file is omitted, Java LiveUpdate looks for its JAR file in the LiveUpdate subdirectory immediately under the Symantec directory. The location of the Symantec directory is specified by the BaseDir parameter in the Symantec Shared section of the Symantec global configuration file /etc/Symantec.conf. Java LiveUpdate returns an error immediately if it cannot locate its JAR file.
urls	The URLs of external Symantec server support. By default, Java LiveUpdate ignores the URL= lines in the TRI file. If this parameter is 1 (true), Java LiveUpdate uses the URL= lines in the TRI file when it uses HTTP to download packages. This parameter and the URL= lines are ignored if FTP is specified as the protocol.
proxy	The name of a proxy server. For example: proxy=addr:port, where the port number is optional. The default port is 80. Addr is the TCP/IP address of the proxy server and :port is the TCP/IP port on which the proxy server is listening (optional). This setting is not supported for FTP.
proxyusername	The user name to use when you log on to the specified proxy server. This setting is needed only if your proxy server requires a logon user name. This setting is not supported for FTP.
proxypassword	The password that is associated with the specified proxyusername account. This setting is needed only if your proxy server requires a logon password. This setting is not supported for FTP.

Table 4-1 liveupdate.conf file parameters

Parameter	Description
maximumLogFileSize	The maximum allowed log file size, in kilobytes (KB). Java LiveUpdate discards older log entries once the log file exceeds the specified maximum size. The default log file size is 1024 KB.
AllowConfigurationOverride	The setting that is used to tell Java LiveUpdate to use the -c command-line parameter and host file setting. If this parameter is set to anything other than True in the shared liveupdate.conf file, Java LiveUpdate ignores the -c parameter and host file setting.
hosts/<host#>/url	The URL of a LiveUpdate server. You may specify a nonstandard port for HTTP servers and a package directory for both FTP and HTTP servers. Java LiveUpdate supports up to 10 servers, starting with 0 through 9. This setting replaces the following Java LiveUpdate 1.10 settings: ■ protocol ■ host ■ packagedir ■ login ■ password
hosts/<host#>/access	The local or mapped directory to access for updates. The path may be a full local path or a UNC share.
hosts/<host#>/login	The user name to use when logging on to a LiveUpdate server using FTP. This optional setting is ignored for all other transports.
hosts/<host#>/password	The password to use when logging on to a LiveUpdate server using FTP. This optional setting is ignored for all other transports.
ConnectionTimeout	The connection time in milliseconds that Java LiveUpdate will wait when it attempts to connect to a LiveUpdate server. The default is 60000 (60 seconds).
ConnectionReadTimeout	The connection timeout in milliseconds that Java LiveUpdate will wait for responses from the LiveUpdate server once a connection has been established. The default is 30000 (30 seconds).
extlog/host#/url=syslog: // <address>[:<port>]	The host address and port of the system log to which Java LiveUpdate sends logs.
extlog/host#/url=sgs	The URL that is used to send logs to Symantec Gateway Security (SGS). This entry may be included only one time in the configuration file.
extlogdest=extlog host#[,extlog/host#]	The list of active external logging services. This setting enables specified external logons if the list is not empty.

Table 4-1 liveupdate.conf file parameters

Parameter	Description
enableSyslogLocalization	The parameter that determines whether to enable localized messages in the syslog. If this parameter is set to YES, localized messages are enabled. The default is NO.

You must specify the working directory on the client computer using the workdir parameter.

Java LiveUpdate must also be able to find its JAR file. For UNIX platforms, Java LiveUpdate searches for jlu.jar in the LiveUpdate subdirectory immediately under the Symantec directory that is specified in /etc/Symantec.conf.

If you want to use a legacy host file, you must type the full path to the host file. The only parameters that are required in the configuration file are the workdir and the hostfile settings. If you are not using a legacy host file, the workdir and the hosts/<host#>/url setting must be specified.

If a setting is followed by :ENC, the value has been encrypted by Java LiveUpdate. The settings that may be encrypted are as follows:

- login
- password
- proxyusername
- proxypassword
- hosts/<host#>/login
- hosts/<host#>/password

Java LiveUpdate 2.0 and later automatically encrypts the login and password settings each time that Java LiveUpdate runs, if the :ENC tag is missing.

Sample liveupdate.conf file

Following is an example of a liveupdate.conf file on UNIX using Java LiveUpdate 2.0 or later:

```
hosts/0/url=http://liveupdate.symanteclive update.com:80

hosts/1/url=http://liveupdate.symantec.com:80

hosts/2/login:ENC=b3effee10d982d2c7449c810c

hosts/2/password:ENC=19d3d3v3c123333898dcf293d

hosts/2/url=ftp://update.symantec.com/opt/content/onramp
```

```
workdir=/tmp

logfile=/opt/Symantec/LiveUpdate/liveupdt.log

jar=/opt/Symantec/LiveUpdate/jlu.jar

urls=1

proxy=proxy.yourcompany.com:8080

proxyusername=joe

proxypassword=geer132

maximumLogFileSize=512

AllowConfigurationOverride=true
```

About configuring proxy settings in Java LiveUpdate

You can configure proxy settings for Java LiveUpdate by changing the following line in the /etc/liveupdate.conf file:

```
proxy=proxy.yourcompany.com:8080
```

To use authentication, you can also edit the following proxyusername and proxypassword lines:

```
proxyusername=MyCompany_user_name

proxypassword=MyCompany_password
```

Configuring Java LiveUpdate to use a Central LiveUpdate server

To set up a Central LiveUpdate server, you need do the following:

- Install LuAdmin.
  For information on how to do this, refer to the *LiveUpdate Administrator's Guide*.

  Note: You must install and run LuAdmin on a Windows 2000 Professional/2003/XP Professional 32-bit, SP 2 computer. It is not available for Linux computers.

- Configure LuAdmin to download the definitions from Symantec onto a Central LiveUpdate server on your network.

Note: Be sure to choose Symantec AntiVirus Virus Definitions under Symantec Product Line when picking the updates to download in LUAdmin.

For information on how to do this, refer to the *LiveUpdate Administrator's Guide*.

- Modify a copy of the liveupdate.conf file to point to your Central LiveUpdate server. You can specify an internal FTP or HTTP server.
- Use any file distribution mechanism to replace the /etc/liveupdate.conf file on each of your Linux client computers with your modified file.

You can configure Java LiveUpdate to use a Central LiveUpdate server by changing one line in the /etc/liveupdate.conf file. You should edit the /hosts/0 line so that the first server checked by your clients is your Central LiveUpdate server.

After you have edited one liveupdate.conf file, you can use any file distribution mechanism to replace the existing /etc/liveupdate.conf file on all your Linux client computers.

To configure the liveupdate.conf file to use a Central LiveUpdate server

- In the liveupdate.conf file, edit the following line to specify the full path to the update definitions directory on your central LiveUpdate server:

  ```
  hosts/0/url=<full path to the update definitions directory on
  the central LiveUpdate server>
  ```

  Be sure to change the hosts/0/ line so that the first place the client checks for updates is your central server.

Wrapping a liveupdate.conf file in an RPM package

If you want to distribute a liveupdate.conf file to all your Linux computers, you can wrap the liveupdate.conf file in an RPM package. Symantec provides a script called make_luconf_rpm.sh and its associated file, luconf.spec, to automate this process. The files are located in the luconfrpm directory.

After you have wrapped the liveupdate.conf file into an RPM package, you can use your RPM distribution to put the liveupdate.conf file into the /etc directory on the Linux computers.

Note: make_luconf_rpm.sh creates an RPM package with the same version number every time. The first time that you run the script, the package installs. Each subsequent time that you run the script and attempt to install it, the RPM package will not install because its version number indicates that this package is already installed.

Each time that you run this script after the first time, you'll need to do one of the following to get the package to install:

- Force the installation using the rpm --force option.
- Edit the luconf.spec script and increment the minor macro number, %define minor, by one.

When you use RPM to install a new liveupdate.conf file that is produced by using this script, RPM first checks to see if there is an existing liveupdate.conf file on the computer. If there is, RPM makes a copy of the file and names it liveupdate.conf.rpm.orig. If you use RPM to uninstall this package, RPM uninstalls the file by changing its name to liveupdate.conf.rpm.save.

To wrap a liveupdate.conf file in an RPM package

1. Create a liveupdate.conf file or edit an existing one.
2. Copy the make_luconf_rpm.sh file from the luconfrpm directory on the Symantec product CD or in your download location to the location where you want to package the liveupdate.conf file. Alternatively, you can copy the file onto a CD and use the /var/tmp directory. You must have write and execute permissions in the directory where you wrap the file.
3. At the command line, type the following:

   <absolute_path>/make_luconf_rpm.sh <absolute_path>/liveupdate.conf

   When typing this command, you must use the fully qualified path for the liveupdate.conf file, even if it is located in the same directory as the script. For example, if you have both the script and the liveupdate.conf file in the same directory and you are in that directory, you can type the following:

   $PWD/make_luconf_rpm.sh $PWD/liveupdate.conf

   The file that is created is named luconf-1.0.0-1.noarch.rpm. It is placed in the root of the current directory.

Enabling Java LiveUpdate logging on Linux servers

By default, a Linux syslog server is not configured to receive messages from remote clients.

In order to receive Java LiveUpdate messages, you must do the following:

- Create a entry in syslog.conf for logging Java LiveUpdate messages.
- Create a messages log file.
- Configure the syslog startup options.
  See "Configuring startup options" on page 64.

If the syslog server is different from the server that is running Java LiveUpdate, you must also modify the firewall to allow inbound traffic on port 514. Finally, you must restart the server for the changes to take effect.

Note: Use tabs, not spaces, when editing the line in the /etc/syslog.conf configuration file.

To create an entry in syslog.conf for logging Java LiveUpdate messages

- In the /etc/syslog.conf configuration file, type **local0.***, and then type the file that you want to send the messages to.
  For example:
  ```
  local0.* /var/log/jlu.log
  ```
  Do not use spaces between local0.* and the name of the file. Use tabs to separate the expressions.

To create a jlu.log file

- At the command line, type the following:
  ```
  touch /var/log/jlu.log
  ```

Configuring startup options

Syslog checks the /etc/syslog.conf file to determine the expected names and locations of the log files that it creates. It also checks the /etc/sysconfig/syslog to determine the various modes in which it should operate. Syslog listens for remote messages when you add the variable -r to SYSLOGD_OPTIONS and -x to disable DNS lookups on messages that are received with -r.

For example:

```
# Options to syslogd
# -m 0 disables 'MARK' messages.
# -r enables logging from remote machines
# -x disables DNS lookups on messages received with -r
# See syslogd(8) for more details
```

```
SYSLOGD_OPTIONS="-m 0 -r -x"

# Options to klogd

# -2 prints all kernel oops messages twice; once for klogd to
decode, and

# once for processing with 'ksymoops'

# -x disables all klogd processing of oops messages entirely

Using Java LiveUpdate 11

Enabling Java LiveUpdate logging on Linux servers

# See klogd(8) for more details

KLOGD_OPTIONS="-2"
```

Note: Make sure that SYSLOGD_OPTIONS contains -r -x.

Configuring firewall rules in /etc/sysconfig/iptables

You need to modify your firewall to allow inbound traffic on UDP port 514. To ensure that you receive only legitimate log entries, you should limit /etc/sysconfig/iptables to the client systems that will send logs to you.

To configure firewall rules in /etc/sysconfig/iptables

1 Do one of the following:

- If you are using Linux, start iptables if necessary, and then add the following rule to be used on the logging server, which is the computer that receives syslog messages:

  -A INPUT -o $IFACE -p udp -s $LOGCLIENT -d $MYIP --dport 514 -j ACCEPT

  In this example, $IFACE is your external ethernet interface (eth0), $MYIP is the IP address of the server that you are adding this iptables rule to, and $LOGCLIENT is the IP address of the computer that sends messages. This rule assumes a default OUTPUT policy of DENY.
- If you are using Red Hat Linux, manually add the following line to the /etc/sysconfig/iptables file:

  -A RH-Lokkit-0-50-INPUT -p udp -m udp --dport 514 -j ACCEPT

  This line should precede any reject lines.

2 Confirm that your iptables configuration file is owned by user root, group root.
For example:
chown root:root /etc/sysconfig/iptables

3 Change the permissions of your iptables configuration file to read/write by user root only.
For example:
chmod 600 /etc/sysconfig/iptables

4 To allow the changes to take effect, do both of the following:
- To restart iptables, at the command line, type the following:
  /etc/init.d/iptables restart
- To restart syslog, at the command line, type the following:
  /etc/init.d/syslog restart

5 To verify that the syslog daemon is running, type the following:
ps -aux | fgrep syslog
The output should be similar to the following:
```
root 1662 0.0 0.0 1576 616 ? S Nov09 0:00 syslogd -m 0
root 18738 0.0 0.0 3664 548 pts/0 S 09:34 0:00 grep -F syslog
```
The first line confirms that the syslog daemon process is up and running; the second line is the command.

Verifying syslog messages

You can use tcpdump to verify that syslog messages arrive at the server.

For example:

tcpdump -a -vv -I -p -c 1000 > tcpdump.log

This configures Linux to run in promiscuous mode so that it receives all messages, logs in ASCII format with increased verbosity to the tcpdump.log file, and then exits after 1000 packets are logged. You can determine if a problem exists on the syslog side, or if a rule is missing for remote logging on a computer that has a firewall.

To verify syslog messages

- At the command line, type the following:
  cat tcpdump.log | grep -v "\^" | grep udp
  This should return values similar to either `. > .514 udp` or `. > .syslog udp`.
  If no Java LiveUpdate messages are making it to the syslog destination, yet the tcpdump log displays lines similar to . > .514 udp or . > .syslog udp, the

problem must be that something other than that the syslog configuration is preventing Java LiveUpdate syslog messages from reaching the syslog target. For example, there may be a firewall on the syslog computer that is blocking the syslog port.

Updating definitions by using Intelligent Updater

Rather than updating virus and security risk definitions by using LiveUpdate on each Linux client computer, you can download an Intelligent Updater shell script. The script has a name in the format yyyymmdd-version-unix.sh, for example, 20050601-008-unix.sh.

The latest Intelligent Updater script is located on the Symantec Security Response Web site at the following URL:

http://securityresponse.symantec.com/avcenter/defs.download.html

For Linux, this script depends on utilities that are distributed as part of the UNIX sharutils package, which must be installed on the computer. It also relies on the UNIX uncompress utility, which is not available on some Linux distributions. If your distribution does not have uncompress, you can work around this issue by creating a symbolic link to the functionally equivalent zcat utility.

Note: The Symantec AntiVirus Linux client computers poll for new definitions every ten minutes. Alternately, you can prompt Symantec AntiVirus to check immediately for new definitions by using symcfg to set the \VirusProtect6\ProductControl\NewPatternFile key to 1.

Downloading and running the script

To use Intelligent Updater, you need to download and run the script.

To download the script

1. Go to the Symantec Security Response Virus Definitions Download Page at the following URL:
   http://securityresponse.symantec.com/avcenter/defs.download.html
2. Select the appropriate Language.
3. Select Symantec AntiVirus Corporate Edition as the product, and then click **Download Updates**.
4. Scroll down to the yyyymmdd-version-unix.sh file, right-click the file, and save it to your computer.

To run the script

1. With the file on the appropriate Linux computer, change the file's permissions to make it executable. For example, type the following:
   ```
   chmod 755 *unix.sh
   ```
2. Double-click the file to run it, or run it from the command line.
   The script then puts the new definitions into the /opt/Symantec/virusdefs/incoming directory.

About updating computers individually

Users can update the virus definitions on a computer using LiveUpdate from the user interface or the command line unless you configure the GRC.DAT file not to allow this.

Chapter 5

Configuring Symantec AntiVirus for Linux

This chapter includes the following topics:

- About configuring clients globally by using a GRC.DAT file
- What you can configure on Linux by using a GRC.DAT file
- Using the Configuration Editor tool
- Deploying GRC.DAT files

About configuring clients globally by using a GRC.DAT file

You can configure Linux client computers globally using GRC.DAT files in the following ways:

- If you have a managed Symantec product environment, you can use the GRC.DAT file that Symantec System Center created on a Windows parent server.
- If you have an unmanaged Symantec product environment, you can use the Configuration Editor tool on a Windows computer that has Symantec AntiVirus installed to create a GRC.DAT file.

You can then copy the GRC.DAT file directly to your Linux client computers or wrap the GRC.DAT file in an RPM package for distribution. The settings that are described in this section take effect on Linux computers regardless of the method you use to produce the GRC.DAT file.

Full documentation for the Symantec System Centerconfiguration settings is located in your *Symantec AntiVirus Administrator's Guide* and in the online Help that is located in the Symantec System Center.

A subset of the configuration settings that are available in the Symantec System Center and the Configuration Editor tool are supported on Linux computers.

See "What you can configure on Linux by using a GRC.DAT file" on page 70.

Configuration by using the Symantec System Center

If you have a managed Symantec product deployment that uses parent servers, you can take the GRC.DAT file from a Windows parent server and deploy it to your Linux client computers. The Symantec AntiVirus Linux client computers recognize the settings in the GRC.DAT file. The GRC.DAT file on a parent server contains the settings you have configured by using the Symantec System Center in your managed environment.

GRC.DAT files are cached by the parent server in the Symantec AntiVirus home directory, typically C:\Program Files\Symantec AntiVirus\GRC.DAT. The GRC.DAT files for client groups can also be used. These are also cached by the parent server in the Symantec AntiVirus home directory, typically C:\Program Files\Symantec AntiVirus\Groups\<client group name>\GRC.DAT.

Configuration by using the Configuration Editor tool

If you have an unmanaged Symantec product deployment, you can manage your Symantec AntiVirus Linux client computers by creating a GRC.DAT file with the Configuration Editor tool. The Configuration Editor tool is located with this product in the \Tools\ConfigEd directory.

Note: The Configuration Editor tool must be run on a Windows computer that has Symantec AntiVirus installed.

What you can configure on Linux by using a GRC.DAT file

The locking of configuration settings is not supported on Linux. By default, a user must have root privileges to make local configuration changes on a Symantec AntiVirus Linux client computer.

Note: Scanning for security risks is not enabled by default in Symantec AntiVirus for Linux, but may be enabled by using the GRC.DAT file. Security risks are then detected and logged, but Symantec AntiVirus cannot take any actions on them.

For scheduled scans, scanning for security risks is set separately for each scheduled scan in the Scan Options dialog box. For manual scans, you can set this option for a single scan to be run as soon as the new GRC.DAT file is processed by checking the Configure client to run a manual scan on grc.dat file processing check box, or you can set it as the default for all subsequent manual scans by unchecking the Configure client to run a manual scan on grc.dat file processing check box.

Table 5-1 describes the supported configuration settings for Linux computers and their locations in the Symantec System Center or the Configuration Editor.

Table 5-1 Supported configuration settings for Linux computers

Setting category	Supported configuration settings	Location
Tray icon	Show Symantec AntiVirus icon on desktop	■ In the Symantec System Center All Tasks > Symantec AntiVirus > Client Administrator Only Options, General tab ■ Not available in Configuration Editor
File System Auto-Protect	Enable Auto-Protect Scan file types by extension Scan for Security Risks Exclude selected files and folders See "About file exclusions" on page 75. Scan Network, Floppy, and CDROM drives	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Client Auto-Protect Options, File System tab ■ In Configuration Editor: Client Auto-Protect Options button, Client Auto-Protect Options dialog box
File System Auto-Protect, Advanced Scan options	Scan files when modified Scan files when accessed or modified Disable file cache Use default file cache size Custom file cache entries	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Client Auto-Protect Options, File System tab, Advanced button ■ In Configuration Editor: Client Auto-Protect Options button, Client Auto-Protect Options dialog box, Advanced button

Table 5-1 Supported configuration settings for Linux computers

Setting category	Supported configuration settings	Location
File System Auto-Protect, Actions	Actions tab: First Actions Actions tab: Second Actions Exceptions tab: Add and configure First and Second actions **Note:** Only the actions for viruses are supported. No actions are supported for security risks.	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Client Auto-Protect Options, File System tab, Actions button ■ In Configuration Editor: Client Auto-Protect Options button, Client Auto-Protect Options dialog box, Actions button
File System Auto-Protect, Notifications	Display notification message on infected computer, and the text field for constructing the message	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Client Auto-Protect Options, File System tab, Notifications button ■ In Configuration Editor: Client Auto-Protect Options button, Client Auto-Protect Options dialog box, Notifications button
Virus Definition Manager	Schedule client for automatic product updates using LiveUpdate Do not allow client to manually launch LiveUpdate	■ In the Symantec System Center: All Tasks > Symantec AntiVirus > Virus Definition Manager ■ In Configuration Editor: Virus Definition Manager button, Virus Definition Manager dialog box
Virus Definition Manager, Advanced Schedule Options	Handle missed events within N days of the scheduled time Perform update within plus or minus N minutes of the scheduled time Randomize the day of the week within the interval beginning on <day> and ending <day>	■ In the Symantec System Center: All Tasks > Symantec AntiVirus > Virus Definition Manager, Advanced button ■ In Configuration Editor: Virus Definition Manager button, Virus Definition Manager dialog box, Advanced button
Scheduled Scans, Scheduled Scans Options	Name Enable scan Frequency When	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Scheduled Scans, Client Scans tab, New or Edit buttons ■ In Configuration Editor: Scheduled Scans button, Scheduled Scans dialog box, New or Edit buttons

Table 5-1 Supported configuration settings for Linux computers

Setting category	Supported configuration settings	Location
Scheduled Scans, Scan Options	File types: All types File types: Selected extensions, Extensions button Enable detection of security risks Exclude files and folders: Exclusion button See "About file exclusions" on page 75.	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Scheduled Scans, Client Scans tab, New or Edit buttons, Scan Settings button ■ In Configuration Editor: Scheduled Scans button, Scheduled Scans dialog box, New or Edit buttons, Scan Settings button
Scheduled Scans, Scan Advanced Options	Scan files inside compressed files If there is a compressed file within a compressed file, expand: N levels deep	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Scheduled Scans, Client Scans tab, New or Edit buttons, Advanced button ■ In Configuration Editor: Scheduled Scans button, Scan Options dialog box, New or Edit buttons, Advanced button
Scheduled Scans, Actions	Actions tab: First Actions Actions tab: Second Actions Exceptions tab: Add and configure First and Second actions **Note:** Only the actions for viruses are supported. No actions are supported for security risks.	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Scheduled Scans, Client Scans tab, New or Edit buttons, Actions button ■ In Configuration Editor: Scheduled Scans button, Scheduled Scans dialog box, New or Edit buttons, Actions button
Scheduled Scans, Notifications	Display notification message on infected computer Text field for constructing the message	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Scheduled Scans, Client Scans tab, New or Edit buttons, Notifications button ■ In Configuration Editor: Scheduled Scans button, Scheduled Scans dialog box, New or Edit buttons, Notifications button

Table 5-1 Supported configuration settings for Linux computers

Setting category	Supported configuration settings	Location
Scheduled Scans, Advanced Schedule Options	Handle missed events within N days of the scheduled time	■ In the Symantec System Center: All tasks > Symantec AntiVirus > Scheduled Scans, Client Scans tab, New or Edit buttons, Advanced button ■ In Configuration Editor: Scheduled Scans button, Scheduled Scans dialog box, New or Edit buttons, Advanced button
Manual Scans, Immediate Manual Scan Options	Configure clients to run a manual scan on GRC.DAT file processing Checking this check box restricts the settings you configure using the Settings button to a single scan to be run as soon as the new GRC.DAT file is processed. Leaving it unchecked makes the settings you configure using the Settings button the default for all subsequent manual scans.	■ Not available from the Symantec System Center ■ In Configuration Editor: Immediate Manual Scan button
Manual Scans, Immediate Manual Scan Options, Settings button	File types: All types File types: Selected extensions, Extensions button Enable detection of security risks Exclude files and folders: Exclusion button See "About file exclusions" on page 75.	■ Not available from the Symantec System Center ■ In Configuration Editor: Immediate Manual Scan button, Settings button
Manual Scans, Scan Advanced Options	Scan files inside compressed files If there is a compressed file within a compressed file, expand: N levels deep	■ Not available from the Symantec System Center ■ In Configuration Editor: Immediate Manual Scan button, Settings button, Advanced button

Table 5-1 Supported configuration settings for Linux computers

Setting category	Supported configuration settings	Location
Manual Scans, Actions	Actions tab: First Actions Actions tab: Second Actions Exceptions tab: Add and configure First and Second actions **Note:** Only the actions for viruses are supported. No actions are supported for security risks.	■ Not available from the Symantec System Center ■ In Configuration Editor: Immediate Manual Scan button, Settings button, Advanced button, Actions button
Manual Scans, Notifications	Display notification message on infected computer Text field for constructing the message	■ Not available from the Symantec System Center ■ In Configuration Editor: Immediate Manual Scan button, Settings button, Advanced button, Notifications button

Note: All other settings in a GRC.DAT file are ignored or unsupported on Linux computers running Symantec AntiVirus.

About file exclusions

In prior versions of the Symantec System Center, file extensions were automatically capitalized to normalize the data for case-insensitive platforms such as Windows and NetWare®. This is also true for prior versions of the Configuration Editor tool.

Note: You must edit the GRC.DAT file manually to add lowercase or mixed-case file extension exclusions to GRC.DAT files that you produced using the Symantec System Center or the Configuration Editor from Symantec AntiVirus 10.0 or earlier. If you are using the Symantec System Center or the Configuration Editor from Symantec AntiVirus 10.1 or later, no manual editing is required.

As there is no version information in the Configuration Editor, the only way to determine which version you are using is to know which version of Symantec AntiVirus you obtained it from.

File extension exclusions should be added to the Exts value in the appropriate scan settings section. For example, to add the extensions xxx and zzz as

exclusions to the scheduled scan named My Linux Scan, you add the text xxx,zzz in the following location:

```
!KEY!=$REGROOT$\LocalScans\ClientServerScheduledScan_XX

...

Exts=Sxxx,zzz

...

ExcludedByExtensions=D1

...

StatusDialogTitle=SMy Linux Scan

...

!KEY!=$REGROOT$\...
```

To add the extensions xxx and zzz as exclusions for AutoProtect, you add the text xxx,zzz in the following in the following location:

```
!KEY!=$REGROOT$\Storages\FileSystem\RealTimeScan

...

Exts=Sxxx,zzz

...

ExcludedByExtensions=D1

...

!KEY!=$REGROOT$\...
```

Using the Configuration Editor tool

The GRC.DAT configuration file provides the configuration information to client machines. Configuration files store important information, such as parent server identity and antivirus server and client configuration settings.

You can use the Configuration Editor to generate a configuration file that can be used with Symantec AntiVirus Linux clients. The tool is located in the /Tools/ConfigEd directory provided as part of your Symantec AntiVirus for Linux software. The tool is named Configed.exe.

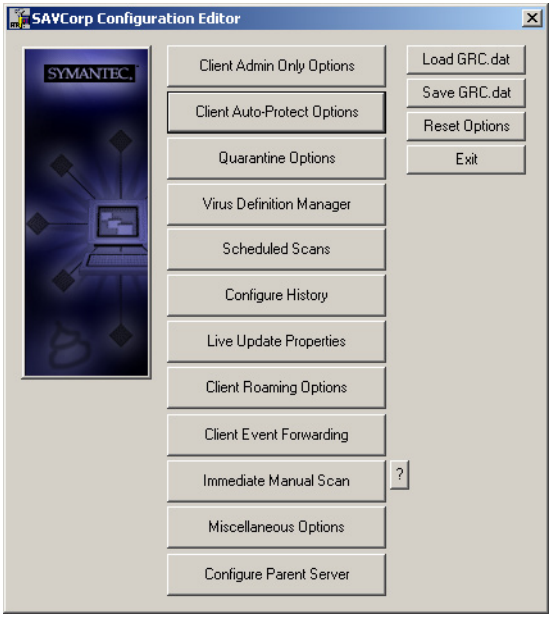
Using the Configuration Editor, you can create various configurations that can be distributed to clients at any time.

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

To start using the Configuration Editor, you need to copy the program onto a Windows desktop.

To copy the Configuration Editor onto the desktop

1. Insert the product CD into your CD ROM drive, or go to your installation download location.
2. Open **Tools > Nosuprt > Configed**.
3. Copy Configed.exe to your Windows desktop.
4. To launch the Configuration Editor, double-click the Configed icon on the Windows desktop.



Creating a configuration file

You can set options with the Configuration Editor and create a new GRC.DAT file with those settings.

To create a configuration file

1. Open the Configuration Editor.
2. Click each option you want to configure from the main Configuration Editor window.
3. When you have finished setting all the options, click **Save GRC.dat**.

Loading and modifying an existing configuration file

You can load an existing GRC.DAT file and edit and save the new settings.

To load and modify an existing configuration file

1. In the main Configuration Editor window, click **Load GRC.dat**.
2. Browse to the existing GRC.DAT file and select it.
3. Click **Open**.

Saving a configuration file

You can save the configuration file that you create either as the default name, GRC.DAT, or with a name that you specify. Before you roll out the configuration file, it must be renamed to GRC.DAT.

To save a configuration file

1. In the main Configuration Editor window, click **Save GRC.dat**.
2. Browse to the directory in which you want to save the file.
3. In the File Name text box, change grc.dat to GRC.DAT.
4. Click **Save**.
   The file must be named GRC.DAT, all in capital letters. You must place this GRC.DAT file in the appropriate /var/Symantec directory on the client computer before it will be processed.

Returning settings to their default configuration

At any time while you are creating or editing a GRC.DAT file, 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**.

Deploying GRC.DAT files

GRC.DAT files are text files that can be edited manually using a text editor. Symantec AntiVirus Linux client computers support GRC.DAT files with either Windows or Linux line endings. The file may not be in Unicode format.

GRC.DAT files are automatically imported every ten minutes. Alternately, administrators can prompt Symantec AntiVirus to import a GRC.DAT file immediately by using the symcfg command line interface to set the value of \VirusProtect6\ProductControl\CheckGRCNow to 1.

Copying a GRC.DAT file

When copying a GRC.DAT file to a Symantec AntiVirus Linux client computer, it is important to remember that the name must be GRC.DAT, all capital letters. The file must be placed into the /var/symantec directory.

To copy a GRC.DAT file

- From the command line, type the following:

  ```
  cp <absolute_path>/GRC.DAT <destination_path>
  ```

Wrapping a GRC.DAT file in an RPM package

If you want to use a GRC.DAT file to configure all your Linux computers, you can wrap the GRC.DAT file in an RPM package. Symantec provides a script that is called make_grcrpm.sh and its associated file, grc.spec, to automate this process. The files are located in the grcrpm directory.

After you have wrapped the GRC.DAT file into an RPM package, you can use your RPM distribution to put the GRC.DAT file into the /var/symantec directory on the Linux computers.

Note: make_grcrpm.sh creates an RPM package with the same version number every time. The first time that you run the script, the package installs. Each subsequent time that you run the script and attempt to install it, the RPM package will not install because its version number indicates that this package is already installed.

Each time that you run this script after the first time, you'll need to do one of the following to make the package install:

- Force the installation using the rpm --force option.
- Edit the grc.spec script and increment the minor macro number, %define minor, by one.

To wrap a GRC.DAT file in an RPM package

1. Create a GRC.DAT file with the configuration that you want by using the Symantec System Center on a Windows parent server, or by using the Configuration Editor tool.
2. Copy the make_grcrpm.sh file from the grcrpm directory on the Symantec product CD or in your download location to the location where you want to package the GRC.DAT file. Alternatively, you can copy the file onto a CD and use the /var/tmp directory. You must have write and execute permissions in the directory where you wrap the file.
3. When typing this command, you must use the fully qualified path for the GRC.DAT file, even if it is located in the same directory as the script. At the command line, type the following:

   <absolute_path>/make_grcrpm.sh <absolute_path>/GRC.DAT

   For example, if you have both the script and the GRC.DAT file in the same directory and you are in that directory, you can type the following:

   $PWD/make_grcrpm.sh $PWD/GRC.DAT

   The file that is created is named grc-1.0.0-1.noarch.rpm. It is placed in the root of the current directory.

Index

A

Auto-Protect
- disabling 33
- enabling 33

C

Configuration Editor
- description 27
- location 76
- using 76

configuration settings
- locking 70
- using the Symantec System Center 70

configuring file exclusions manually 75

G

Gnome desktop environment 17
GRC.DAT file
- copying 79
- creating 77
- deploying 79
- editing manually 75
- loading and modifying 78
- locations 70
- producing 76
- saving 78
- settings supported on Linux 70
- using the Configuration Editor tool 70
- wrapping in an RPM package 62, 79

I

installing
- locally 22
- remotely 23
- scenarios 20

Intelligent Updater
- description 67
- downloading and running 67

J

Java LiveUpdate 57
- configuring logging 63
- configuring to use central server 61
- encryption 60
- proxy settings 61
- using the sav liveupdate command 33

Java Runtime Environment 17
jlu.jar 60

K

KDE desktop environment 17
kernels, supported 17

L

LiveUpdate Administration Utility. *See* LuAdmin
liveupdate.conf
- file 58
- parameters 58
- sample 60

log facilities 46, 51
log severity levels 47, 51
LuAdmin
- description 56
- files 57

luau.exe 56

M

make_grcrpm.sh script 62, 79

P

packages
- dependencies 19
- name format 19

R

requirements
- hardware 16

requirements *(continued)*
    software 17
RPM 19, 23
rtvscand service
    description 27, 47
    syntax 51

S

sav command-line interface
    description 26, 28
    syntax 28
    using 33
sav package 19
savap package 20
savjlu package 20
savtray command-line interface, description 27
savui package 20
semaphores 43
software distributions 17
symcfg command-line interface
    description 26, 40
    syntax 40
    using 42
symcfgd service
    configuration parameters 44
    description 27, 43
    interacting with 45
    syntax 47
system requirements 16, 17

U

uninstalling 23

X

X11 application 17