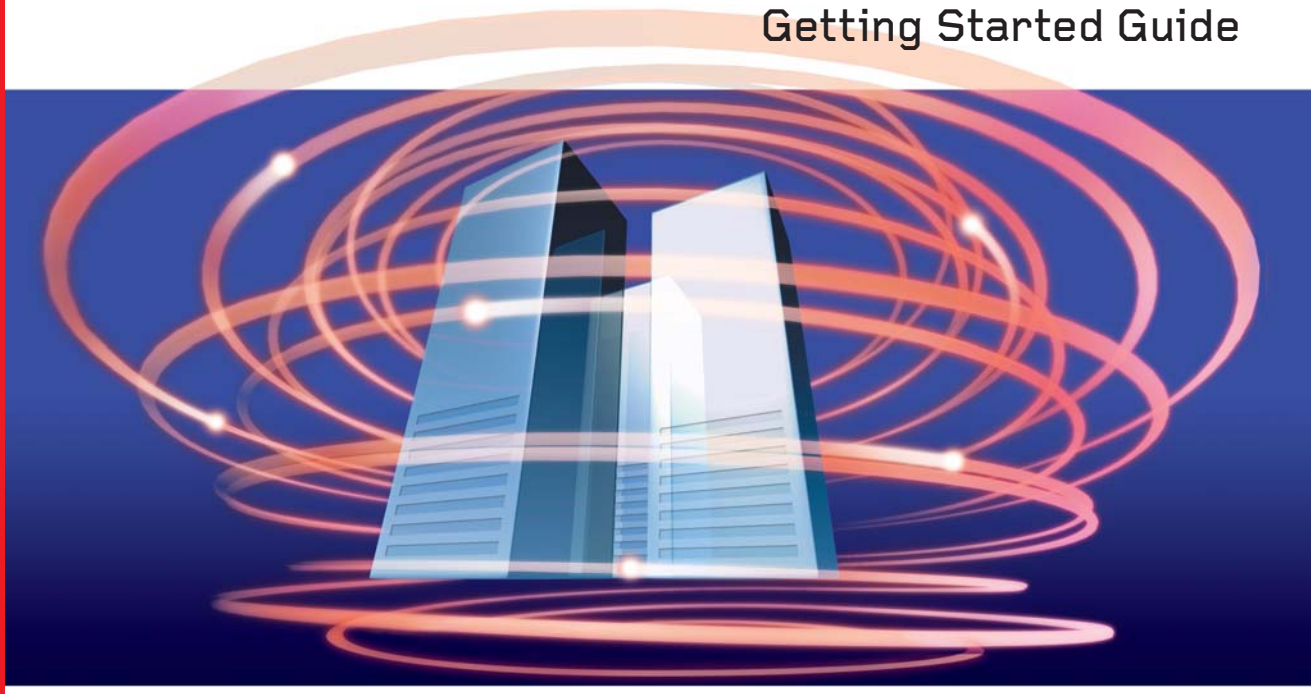
TREND MICRO™
ServerProtect™ 2
Stops Viruses from Spreading through Linux Servers

for Linux ™

Getting Started Guide



TREND MICRO™

Document Part No. SPEM22345/50715

Release Date: April 2006

Protected by U.S. Patent No. 5,951,698

The Getting Started Guide for Trend Micro™ ServerProtect™ for Linux™ is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

For technical support, please refer to chapter 5, Troubleshooting and Contacting Technical Support, for technical support information and contact details. Detailed information about how to use specific features within the software are available in the online help file and online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

`http://www.trendmicro.com/download/documentation/rating.asp`

Contents

Chapter 2: Installing ServerProtect for Linux—continued

Chapter 3: Getting Started with ServerProtect

Chapter 4: Configuring and Performing Scans with ServerProtect

Chapter 4: Configuring and Performing Scans with ServerProtect—continued

Chapter 5: Troubleshooting and Contacting Technical Support

Chapter 1

Introducing ServerProtect™ for Linux™

Trend Micro ServerProtect for Linux provides comprehensive protection against computer viruses, Trojans, and worms for file servers based on the Linux operating system. Managed through an intuitive portable Web-based console, ServerProtect provides centralized virus scanning, pattern updates, event reporting and antivirus configuration.

This chapter discusses the following topics:

Protecting Linux Servers

ServerProtect for Linux scans data and executable files on Linux systems to detect and protect against viruses, worms, Trojans, and spyware/grayware. While Linux systems are less vulnerable than Windows systems, they are not immune. Many Linux systems are used as file servers for Windows-based systems. Without protection against viruses and other security risks at the server level, Windows threats may quickly spread across the network.

And, the increase in popularity of the Linux platform has resulted in the growth of viruses and other malware specifically targeting Linux servers. Viruses that attack the Linux platform are becoming more frequent and severe.

Quarantines

Quarantines are areas on your computer or network where files that cannot be cleaned are stored. The messages or files may eventually be deleted, to limit the storage space needed by the quarantine.

One important use of quarantines is to temporarily store files that contain malicious code. With quarantined files, unlike deleted files, if the actual contents of the file are needed later, they can be recovered. Administrators can use the quarantine aggressively without concern that important information will be permanently lost.

Platforms, Compression, and Encoding

Trend Micro has developed scan engines for all major platforms, including Windows, Unix, and DOS (individual platforms are listed below). In addition, the scan engines recognize all file types, more than 20 compression types, major encoding algorithms, Microsoft™ Office macros, and Web scripting languages. No known viruses or network exploits get past the engine, and there are multiple layers of analysis and protection that guard against unknown threats.

Password Protected/Encrypted Files

Since ServerProtect must open a file to scan it, ServerProtect cannot scan password-protected or encrypted files. The ServerProtect scan engine recognizes these files as unable to be opened (and therefore un-scannable). The administrator can designate all such files for automatic quarantine or choose to have the scan engine ignore these files.

Platforms That ServerProtect Can Scan

Platform	Version	
UNIX	Solaris™ Linux (all major distributions)	IBM AS/400 OS/390
Microsoft Windows (SPLX management console)	Windows™ 2003 Windows NT 3.5 Windows Me Windows 95	Windows NT 4.x Windows XP Windows 98
DOS	(all versions)	

Encoding

- MIME
- UUencode
- Bin/Hex

File Types

- Executables, including `.exe`, `.com`, `.lnk`, `.bas`, and `.reg`
- Library files, including `.dll`
- Others, including `.hlp` and `.chm`
- Microsoft Office files (see *Macro Scripts*, below)

Compression

- Tar
- Gzip
- All windows compression formats

Macro Scripts

- WordBasic
- VBA (Visual Basic for Applications)
- VBA3

Note: Examples of applications that host Macro scripts are Microsoft Word and Excel, OpenOffice, and Rexx.

Scripting Languages

- JavaScript
- VBScript

Understanding How ServerProtect for Linux Works

ServerProtect software provides real-time, manual, and scheduled antivirus scanning for Linux servers. ServerProtect protects SAMBA file-sharing, HTTP, and FTP traffic by detecting and removing viruses and other security risks from files (including compressed files) before they reach end users.

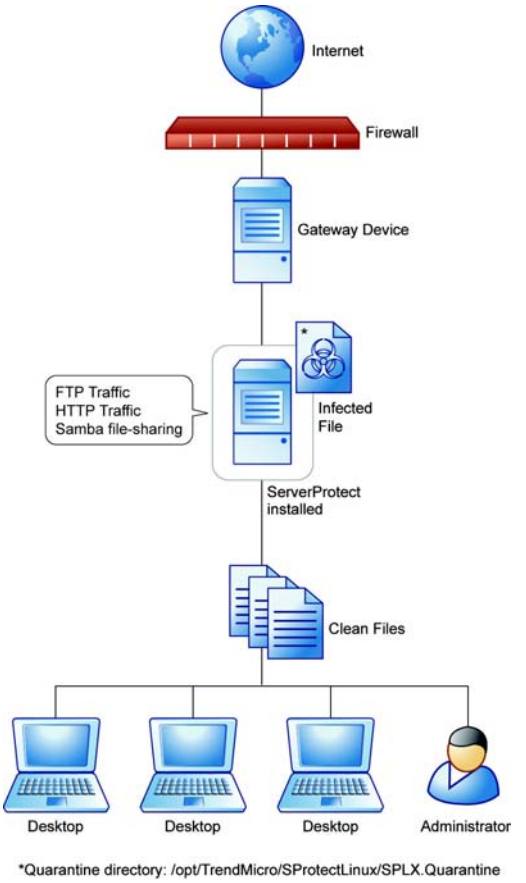


FIGURE 1-1. How ServerProtect works

ServerProtect offers a Web-based console that allows for easy remote access from any location with an Internet connection. Command-line alternatives are available for many features of the application. You can configure notifications to alert you when system events or an attempted attack has taken place.

Exploring ServerProtect Scanning Technologies

ServerProtect for Linux uses the following technologies to detect different forms of malicious software (malware): pattern matching, MacroTrap™, ScriptTrap™, and compressed file scanning.

Pattern Matching

ServerProtect draws upon an extensive database of virus patterns to identify viruses and other malware through a process called “pattern matching.” ServerProtect examines key areas of suspect files for telltale strings of malware code and then compares them with thousands of virus signatures that Trend Micro has on record.

For polymorphic or mutating viruses, the ServerProtect scan engine permits suspicious files to execute in a protected area for decryption. ServerProtect then scans the entire file, and looks for strings of mutation-virus code.

WARNING! *Due to the large number of new viruses, always keep the virus pattern file up-to-date.*

MacroTrap

Macro viruses are application-specific; which means they can attack multiple operating systems. Given this cross-platform compatibility, combined with the popularity of the Internet and increasing power of macro languages, the magnitude of the threat posed by these viruses is obvious. Trend Micro’s MacroTrap provides you with a means of protecting your network from this type of malware.

How MacroTrap Works

MacroTrap performs a rule-based examination of all macro code associated with a document. Macro virus code is typically contained as part of an invisible template (for example, *.dot in Microsoft Word) that travels with the document. MacroTrap checks the template for signs of a macro virus by seeking out instructions that

perform virus-like activity. Examples of this behavior include copying parts of the template to other templates (replication), and execution of harmful commands (destruction).

Compressed File Scanning

Compressed files and archives are the preferred file formats for distribution by way of email or the Internet. Unless your antivirus application is specially equipped to handle these files, viruses and other security risks may be “smuggled” into your network inside these files.

The ServerProtect scan engine scans inside archives and compressed files, and can even detect viruses in compressed files and archives composed of other compressed files - up to twenty (20) compression layers deep, if so configured. If ServerProtect scans a file more than 20 layers deep, layers 21+ are “skipped” but are recorded in the system logs.

The Trend Micro scan engine can detect malware in archives created by popular compression and archival algorithms, such as *.zip, *.arj, *.lzh. A comprehensive list is available in the *How ServerProtect Finds Viruses* topic in the online help.

Compressed File Scan Limit

To help conserve system resources, you can configure ServerProtect to scan files within compressed archives that do not exceed a specific size. Skipped compressed files appear in the system logs. It is important to note that the smaller the size specified, the higher the risk of infection.

Note: The Real-time Scan option still detects viruses included in skipped files during a decompression attempt.

ServerProtect for Linux Features

The following are noteworthy features of ServerProtect for Linux:

Reports Available from Control Manager

Because you can now manage ServerProtect from Trend Micro Control Manager (TMCM), the following reports are now available:

- Top 10 virus Detection Points report
- All Entities Virus Infection List
- Top 10 Infected Files Report
- Top 10 Viruses Report

The TMCM server consolidates these reports from log data, so these reports are available only when managing ServerProtect from TMCM.

Multiple-Processor Support

ServerProtect can be installed on both single and multiple-processor servers.

Remote Management Through a Web Browser

You can configure ServerProtect for Linux via a browser-based console. This allows you to control the application from any location. You can configure ServerProtect for Linux via a browser-based console using Microsoft™ Internet Explorer™, Mozilla™, or Mozilla Firefox.

Manual, Real-Time, and Scheduled Scanning

In addition to on-demand scanning (the “Scan Now” option), ServerProtect can act against viruses automatically without user intervention. Whenever you access a file, real-time scan checks that file for viruses (for example, when you copy or open a file). Scheduled scanning performs a thorough scan of your Linux machine at regular, user-specified intervals. Schedule scans after office hours to avoid interfering with normal operations.

Backup Directory Configuration

ServerProtect can back up infected files before the Real-time Scan, Scan Now, or Scheduled Scan features performs the Clean action. This is useful when an infected file cannot be cleaned and as a result it is not recoverable.

Detailed, Easy-to-Maintain Logs

You can view and export comprehensive logs about system and/or antivirus activities performed on your system. ServerProtect also allows you to delete logs automatically, to keep them from becoming excessively large.

Manual and Automated Log Deletion Options

You can delete logs on-demand and according to a schedule.

Manual or Automated Internet-Based Updates

Perform manual or scheduled virus pattern and scan engine file updates to ensure up-to-date virus protection. ServerProtect even gives you the option to specify your Internet-based update server. To set up your own update server, contact Trend Micro technical support.

Character Set Selection for Email Notifications

You can specify the appropriate character set for your email notifications using a convenient drop-down menu. See Figure 1-2. *Preferred character sets available with ServerProtect* on page 1-9 for available character sets.

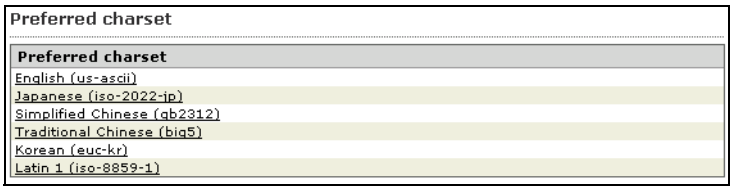


FIGURE 1-2. Preferred character sets available with ServerProtect

Notification of Virus Outbreaks

You can configure email and/or Simple Network Management Protocol (SNMP) notifications about events, such as virus outbreaks, that occur on machines running ServerProtect.

Outbreak Prevention Services

Outbreak Prevention Services (OPS) are Trend Micro services that you can take advantage of when using Control Manager. OPS enables enterprises to take proactive steps against new virus threats before the necessary virus pattern files are available. By bridging the gap between threat notification and virus pattern delivery, enterprises

can quickly contain virus outbreaks, minimize system damage, and prevent undue downtime.

When registered to Trend Micro Control Manager, ServerProtect can take advantage of OPS for file blocking.

OPS is a key component of the Trend Micro Enterprise Protection Strategy (EPS), the culmination of a research initiative that identified best practices for preventing or deflecting potentially damaging virus attacks. This study was brought on by the apparent failure of conventional security measures to defend against new generation threats, such as CodeRed and Nimda.

Trend Micro created Outbreak Prevention Services to address concerns at each stage of the outbreak life cycle. OPS harnesses the three core strengths of Trend Micro:

- Enterprise-class antivirus and content security products
- TrendLabs, the Trend Micro ISO-certified virus research and technical support center
- Partnerships with best-of-breed network security vendors

...and brings them together in a single powerful interface: Trend Micro Control Manager.

With OPS, Control Manager provides answers to the following key security questions:

- Am I under attack?
- Can my system handle the attack?
- How should I respond to the attack?

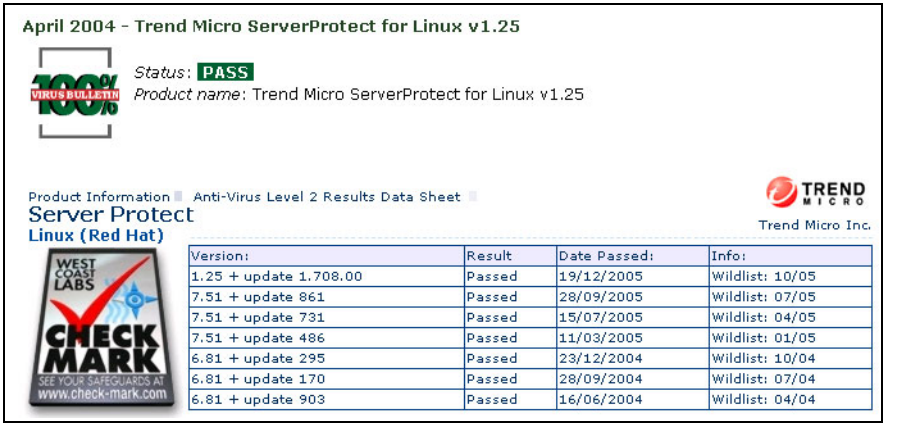
Note: For additional information on the Enterprise Protection Strategy, visit the Trend Micro Web site at `http://www.trendmicro.com`.

ServerProtect for Linux Benefits

The following are noteworthy benefits of ServerProtect for Linux:

Award-Winning Software

ServerProtect is a proven award-winning product:


April 2004 - Trend Micro ServerProtect for Linux v1.25

Status: PASS

Product name: Trend Micro ServerProtect for Linux v1.25

Product Information | Anti-Virus Level 2 Results Data Sheet

Server Protect

Linux (Red Hat)

Trend Micro Inc.

Version:	Result	Date Passed:	Info:
1.25 + update 1.708.00	Passed	19/12/2005	Wildlist: 10/05
7.51 + update 861	Passed	28/09/2005	Wildlist: 07/05
7.51 + update 731	Passed	15/07/2005	Wildlist: 04/05
7.51 + update 486	Passed	11/03/2005	Wildlist: 01/05
6.81 + update 295	Passed	23/12/2004	Wildlist: 10/04
6.81 + update 170	Passed	28/09/2004	Wildlist: 07/04
6.81 + update 903	Passed	16/06/2004	Wildlist: 04/04

FIGURE 1-3. ServerProtect awards and recognition

Application Execution Protection

ServerProtect's Real-time Scan option detects viruses in Linux applications whenever an application is executed. See *Configuring Real-Time Scanning* starting on page 4-9 for additional information.

Command-Line Interface Support

In addition to providing a Web-based management console, ServerProtect provides command-line support for the following: real-time scans, scheduled scans, manual scans, notifications, log deletions, and virus pattern/engine updates. See Appendix A, *Understanding tmsplx.xml* starting on page A-2, for information about command line options.

Backup Directory Configuration

ServerProtect can back up infected files before the Real-Time Scan, Scan Now, or Scheduled Scan options perform the Clean action. As a precaution, you may want to create backup copies of your files.

Detailed Exportable Logs

You can view and export comprehensive logs about system and/or antivirus activities performed on your system.

Support for Advanced ActiveUpdate Options

Edit `tmsplx.xml` to enable or disable advanced options for ActiveUpdate. Refer to the ServerProtect Web-based console online help topic *Enable/Disable Advanced ActiveUpdate Options* for details.

The component update feature provides the following options:

Digital signature checking – ServerProtect can implement this feature (disabled by default) whenever it downloads components from the Trend Micro ActiveUpdate server

Secure Sockets Layer (SSL) support – ServerProtect supports secure component download either from the Trend Micro ActiveUpdate server or from your company's update server

Server authentication support – ServerProtect supports HTTPS authentication when downloading components from an HTTPS source

Support for other types of proxy servers – ServerProtect supports the following proxy server types and authentication methods:

- Squid proxy with basic authentication (both HTTP and SSL)
- Squid with digest authentication (both HTTP and SSL)

Consistency Checking Between ServerProtect Web Console and Configuration File (`tmsplx.xml`)

ServerProtect performs a consistency check between the Web console and configuration file (`tmsplx.xml`) for certain ServerProtect options. When a `tmsplx.xml` option is modified manually (for example, using `vi`), the following message displays:

The splx configuration file /opt/TrendMicro/SProtectLinux/tmsplx.xml was previously modified by another program...

Support for New Virus Pattern File-Numbering Format

ServerProtect 2.5 uses the pattern file-numbering format `n.nnn.nn` introduced in version 1.3 of ServerProtect. Under this system, the first 4 digits represent the pattern file number and the last two digits represent the number of the file build or its controlled release version.

Support for Intel™ Hyper-Threading Technology

You can install ServerProtect on servers running Intel's Hyper-Threading Technology. Please refer to the Intel Web site for more details on this technology.

Support for Trend Micro Online Registration System

Use your Registration Key to register ServerProtect and obtain a serial number on the Trend Micro Registration Web site.

`https://olr.trendmicro.com/registration/`

Options for Detailed Debugging

ServerProtect provides the following debug options:

Kernel debugging – debugs kernel-related actions

User debugging – debugs user-related actions

Control Manager debugging – debugs Trend Micro Control Manager-related actions

See *Enabling Debug Logs* starting on page 5-4 for details.

Support for Multiple Update Servers

You can set up backup update servers to provide virus pattern and engine updates (as a fail-over) if the primary update server is not available. See *Configuring a Manual Update* starting on page 3-13, *Configuring Scheduled Updates* starting on page 3-16, and *Manual or Automated Internet-Based Updates* starting on page 1-9 for more information.

HTTPS (SSL) Support

You can access the ServerProtect Web-based console using the HTTPS protocol. See *To access the Web console:* starting on page 3-10 for configuration information. SSL (Secure Sockets Layer) secures a communication channel between a Web browser and a host server. You can take advantage of this protocol to manage ServerProtect without jeopardizing security policies.

Quick Access Graphical User Interface Console for XWindow

The Quick Access console is available for managing ServerProtect on the Konqueror Desktop Environment (KDE) graphical desktop environment. Use the KDE Quick Access console to:

- Start/stop manual scanning (Scan Now).
- Start/stop ServerProtect services and httpd.
- Launch the Web console.
- Delete logs manually.
- Start a manual update (Update Now).
- Stop a scheduled scan.

To access the Quick Access console

1. Log on as a *root*.
2. From the task bar on the XWindow main window, click **Start Applications Menu** > **System (Tools)** > **TrendMicro SPLX Administration**.

Use this console to:

- Start/stop manual scanning (Scan Now). See *Invoking Manual Scan (Scan Now)* starting on page 4-12 for more information.
- Start/stop ServerProtect. See *Accessing ServerProtect Using the Quick Access Console Menus* starting on page 3-2 and *Using splx Script* starting on page A-34 for more information.
- Launch the Web console. See *Using the ServerProtect Web Console* starting on page 3-10 for more information.
- Delete logs manually. This is equivalent to the `splxmain -g` command. See *Using splxmain* starting on page A-30 for more information.
- Start a manual update (Update Now). See *Invoking Manual Scan (Scan Now)* starting on page 4-12.
- Stop a scheduled scan. See *Stopping a Scheduled Scan* starting on page 4-16 for more information.

What's New in ServerProtect for Linux

For customers who are familiar with previous versions of Server Protect for Linux, the following new features are available in version 2.5:

Manage ServerProtect with Trend Micro Control Manager™

For the first time, you can use the Trend Micro central management console, Trend Micro Control Manager (TMCM), to manage ServerProtect for Linux. You can do so because of the new, HTTP-based protocol introduced in TMCM 3.5. When registered to TMCM, ServerProtect can make use of TMCM features such as

- Reports are available from Trend Micro Control Manager. See *Reports Available from Control Manager* on page 1-8.
- Outbreak Prevention Services (for file blocking). See *Outbreak Prevention Services* on page 1-9.

Remote Installation

You can install one or multiple instances of ServerProtect to remote machines by using the new RemoteInstall tool.

A New Online Help Architecture

This release includes a new online help architecture for ServerProtect. It has been thoroughly tested for usability and customer needs.

In addition to the above new features, the following features are available in version 2.5:

Support for New Platforms

In this release, supported platforms are based on the Linux kernel 2.6. The supported platforms are:

- Red Hat Enterprise Linux 4 (including AS, ES, and WS)
- SUSE Enterprise Linux Server 9
- Novell Linux Desktop 9
- Debian 3.1

One Binary Package for All Supported Linux Distributions

Previous versions of ServerProtect for Linux required a separate installation process, depending on the platform. As of release 2.5, installation has been simplified and only one installation package is required for all supported platforms.

Automatic Start of Expiration Control Countdown

In previous versions of ServerProtect, you had to log on to begin the countdown of your product expiration period. In version 2.5, expiration countdown automatically begins as soon as the ServerProtect service starts.

Support for Wildcards with Exclusion Directory

The include and exclude scanning paths for Real-time, Scheduled, and Manual Scans now support the use of the asterisk (*) and the question mark (?) wildcards. An asterisk (*) wildcard matches any number of characters, and a question mark (?) wildcard matches only one character.

IntelliScan and ActiveAction Technology

New technology is available in this release of ServerProtect:

IntelliScan - IntelliScan is a new method of selecting the files to be scanned, in addition to Scan All or Scan by File Name Extension. IntelliScan optimizes security by examining file headers using true file type recognition, and scanning file types known to potentially harbor malicious code.

ActiveAction - ActiveAction is a new method of selecting the action to take when a security risk has been detected. Trend Micro customizes scan actions for different types of security risks. New scan actions are updated when you download new pattern files from Trend Micro.

Option To Exclude Network-Mounted Drives From Scanning

You may have network file systems that you want to exclude from scanning. Now you can exclude these mapped drives from Manual and Scheduled Scanning. See the online help topics titled *Configuring a Manual Scan* and *Configuring a Scheduled Scan* for more information.

Safer Configuration File Modifications

In release 2.5, ServerProtect now provides error-checking for changes to the configuration file. You can also recover easily from mistakes with a backup configuration file that lets you roll back to the previous version if needed.

Ability to Perform ActiveUpdates at Random Intervals

To help control peak usage of the ActiveUpdate server network bandwidth, ServerProtect offers the ability to randomly perform updates within a specified time period, following a scheduled update start date and time.

An Improved User Interface

If you are familiar with previous versions of ServerProtect, you may notice that version 2.5 has a new look and feel. The banner colors and appearance have changed, and the overall design of the user interface has been enhanced. For example:

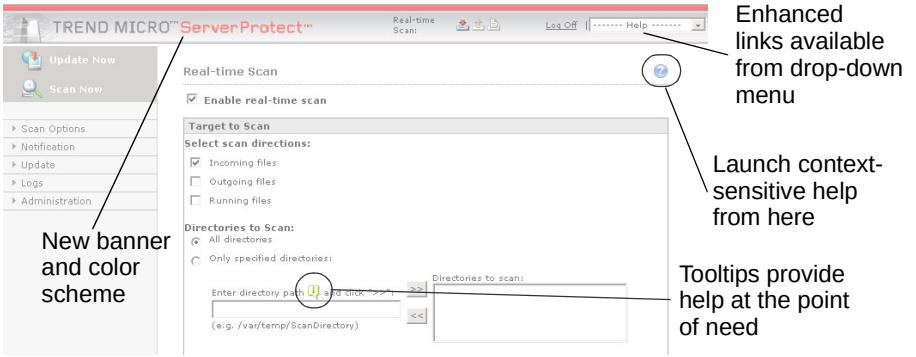


FIGURE 1-4. Enhanced user interface is available in version 2.5

Using the Product Documentation

The documentation set for this product includes the following:

- **Getting Started Guide**—This Guide helps you get "up and running" by introducing ServerProtect, assisting with installation planning, implementation, and configuration, and describing the main product functions. It also includes instructions on testing your installation using a harmless test virus. The latest version of the Guide is available in electronic form at:

  `http://www.trendmicro.com/download/`

- **Online help**—The purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values. Online help is accessible from the ServerProtect management console.
- **Man pages**—ServerProtect for Linux provides manpages for the splxmain, splx, tmsplx.xml, RemoteInstall, and CMconfig files. See *Accessing ServerProtect Man Pages* starting on page A-2 for more information.
- **Readme file**—The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and release history.
- **Knowledge Base**— The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  `http://esupport.trendmicro.com/`

Chapter 2

Installing ServerProtect for Linux

Here you will find instructions for installing, registering, activating, and removing ServerProtect for Linux 2.5. This chapter discusses the following topics:

System Requirements

Servers on which you install ServerProtect must meet the following requirements.

Hardware

CPU

- Intel™ Pentium™ II processor (or higher)
- AMD™ Athlon™ processor

Memory

- 256MB or more (512MB recommended for application/file servers)

Disk space

- 50MB for the `/opt` directory
- 50MB for the `/tmp` directory

Software

Supported Distributions and Kernels

- Red Hat™ Enterprise Linux (AS, ES, WS) 4.0
    - 2.6.9-5.EL up
    - 2.6.9-5.EL smp
    - 2.6.9-22.EL up
    - 2.6.9-22.EL smp
    - 2.6.9-22.0.2.EL up
    - 2.6.9-22.0.2.EL smp
- SUSE™ LINUX Enterprise Server 9
    - 2.6.5-7.97 up
    - 2.6.5-7.97 smp
    - 2.6.5-7.244 up
    - 2.6.5-7.244 smp

- Novell™ Linux Desktop 9
  - 2.6.5-7.111 up
  - 2.6.5-7.111 smp
  - 2.6.5-7.244 up
  - 2.6.5-7.244 smp
- Debian 3.1
  - 2.6.8-2_16 up
  - 2.6.8-2_16 smp

Note: The Debian platform requires the `libstdc++-2.10-glibc2.2_i386.deb` 2.9x version package.

For other kernels and distributions, refer to the following Web site for additional information: `http://www.trendmicro.com/en/products/file-server/sp-linux/use/kernel.htm`

Supported XWindow Graphical Desktop Environments

To use Quick Access console menus and command-line alternatives, install:

- Konqueror Desktop Environment (KDE) 3.2 or 3.3

Note: The Quick Access console is available only when you are logged on as *root*. XWindows does not support root login on the Debian 3.1 default platform.

Note that the Gnome desktop environment is not supported.

Supported Web Browsers

Access the ServerProtect 2.5 Web console through the following browsers:

- Microsoft™ Internet Explorer™ 5.5 or above with Service Pack 2
- Mozilla 1.6 - requires Sun Micro Java Runtime Environment 1.4.2_01 (or any release up to 1.5.0_02)
- Mozilla Firefox 1.0 - requires the Sun Micro Java 2 Runtime Environment (JRE) 1.4.2_01 (or any release up to 1.5.0_02)

If you have not installed the JRE, the logon screen appears as shown in the following example.

FIGURE 2-1. Logon screen when users accessing the Web console with Mozilla browsers have not installed the JRE

To enable the Java plug-in, go to the Mozilla plug-in directory and then create a symbolic link to the Java plug-in. For example:

```
# cd /usr/lib/mozilla/plugins
# ln -s \
# /usr/java/j2re1.4.2/plugin/i386/ns610-gcc32\
# libjavaplugin_oji.so libjavaplugin.so
```

Upgrading from Previous Versions

ServerProtect 2.5 is a major release, and no migration path is available from ServerProtect 1.3.x or earlier. Remove prior versions from your server before installing ServerProtect 2.5. See *Removing ServerProtect* starting on page 2-30 for more information.

Running the ServerProtect Installation Program

Before installing ServerProtect for Linux, verify that your Linux distribution and kernel are supported by this release. (See *Supported Distributions and Kernels* on page 2-2). If your distribution and kernel are not listed in the System Requirements section of this chapter, you may need to first install the Kernel Hook Module (KHM) that corresponds to your Linux system.

Kernel Hook Module

This version of ServerProtect for Linux comes prepackaged with a kernel hook module (KHM) for each of the supported kernels. Installation of a kernel hook module is required for ServerProtect to perform real-time scanning for viruses and malicious code. If your environment is one of those listed in the "System Requirements" section of this chapter (see *Supported Distributions and Kernels* on page 2-2), you can use one of the KHMs that come prepackaged with ServerProtect.

Otherwise, after you install ServerProtect, you can conveniently download the version of the KHM that you need from the Trend Micro ServerProtect for Linux Kernel Support Web site:

`http://www.trendmicro.com/en/products/file-server/sp-linux/use/kernel.htm`

For instructions on installing a KHM, see *Installing a Kernel Hook Module* on page 2-31.

Note: During installation, if you receive an error message that a dependent package must be installed to continue the installation, install the required package before proceeding.

License Agreement

After beginning the installation of ServerProtect, the first task is to review and accept the license agreement.

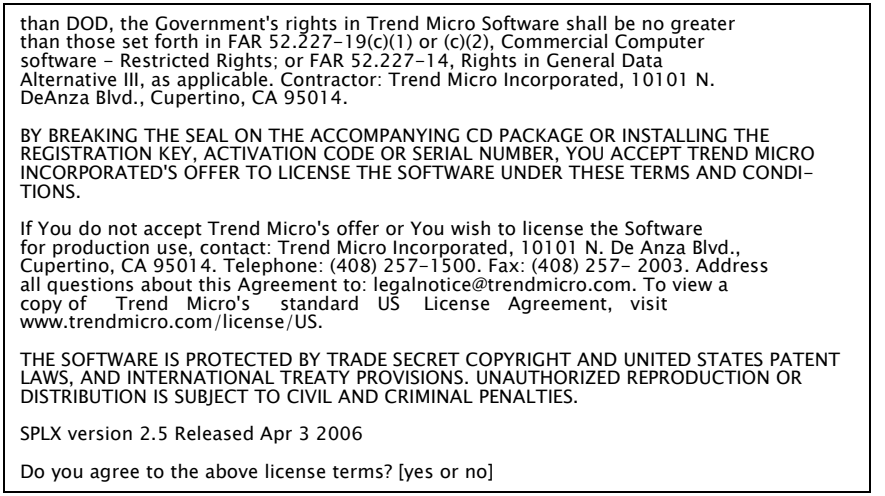
To begin ServerProtect installation:

1. Download or copy the ServerProtect for Linux installation files.
2. Log on as *root*.
3. From the directory containing the ServerProtect for Linux installation files, type the following at the command line:

```
# ./SProtectLinux-2.5.i686.bin
```

Note: The above command extracts the required files to their proper locations.

4. The Trend Micro End User License Agreement displays. Scroll to review the license. When you have finished viewing, type "yes" to accept the licensing terms. (If you do not click "yes," installation cannot continue.)



than DOD, the Government's rights in Trend Micro Software shall be no greater than those set forth in FAR 52.227-19(c)(1) or (c)(2), Commercial Computer software - Restricted Rights; or FAR 52.227-14, Rights in General Data Alternative III, as applicable. Contractor: Trend Micro Incorporated, 10101 N. DeAnza Blvd., Cupertino, CA 95014.

BY BREAKING THE SEAL ON THE ACCOMPANYING CD PACKAGE OR INSTALLING THE REGISTRATION KEY, ACTIVATION CODE OR SERIAL NUMBER, YOU ACCEPT TREND MICRO INCORPORATED'S OFFER TO LICENSE THE SOFTWARE UNDER THESE TERMS AND CONDITIONS.

If You do not accept Trend Micro's offer or You wish to license the Software for production use, contact: Trend Micro Incorporated, 10101 N. De Anza Blvd., Cupertino, CA 95014. Telephone: (408) 257-1500. Fax: (408) 257- 2003. Address all questions about this Agreement to: legalnotice@trendmicro.com. To view a copy of Trend Micro's standard US License Agreement, visit www.trendmicro.com/license/US.

THE SOFTWARE IS PROTECTED BY TRADE SECRET COPYRIGHT AND UNITED STATES PATENT LAWS, AND INTERNATIONAL TREATY PROVISIONS. UNAUTHORIZED REPRODUCTION OR DISTRIBUTION IS SUBJECT TO CIVIL AND CRIMINAL PENALTIES.

SPLX version 2.5 Released Apr 3 2006

Do you agree to the above license terms? [yes or no]

FIGURE 2-2. License agreement acceptance

5. ServerProtect installs, typically within minutes. When the installation is complete, ServerProtect asks if you want to register your ServerProtect server to Trend Micro Control Manager:

   ```
   Do you wish to connect this SPLX server to Trend Micro
   Control Manager? (y/n) [y]
   ```

6. If you do not wish to manage ServerProtect by using Control Manager, type n and press Enter. An "installation complete" message displays and ServerProtect asks if you would like to enter your activation code. See *Activating ServerProtect During Installation* on page 2-9 for further guidance on this process.

Setting Up ServerProtect for Use with Control Manager

If you would like to manage ServerProtect through Trend Micro Control Manager, follow the procedures described below during installation.

Registering ServerProtect to Trend Micro Control Manager

With this release of ServerProtect, for the first time you can manage ServerProtect by way of Trend Micro Control Manager. Registering to Control Manager is part of the ServerProtect installation process.

To register ServerProtect to Control Manager:

1. Begin the ServerProtect installation as described in *To begin ServerProtect installation:* on page 2-6.
2. When the installer asks, "`Do you wish to connect this SPLX server to Trend Micro Control Manager?`", type **`y`** and press **ENTER** (or just press **ENTER** to accept the default of **`y`**). The installer displays a message saying that it will now collect necessary data from you and displays a list of available IP addresses for your ServerProtect server.
3. At the `IP of SPLX machine:` prompt, enter the IP address of your ServerProtect server. The installer stores your server IP address and prompts you for your Control Manager server IP address.
4. At the `Control Manager server IP:` prompt, enter the IP address of the Trend Micro Control Manager server that you want to use to manage ServerProtect. The installer stores your Control Manager IP address and prompts you for your Control Manager port.

5. At the `Control Manager server port: [80]`, enter the number of the port that you would like to use to access Control Manager or just press **ENTER** to accept the default value of 80. The installer stores your port number and asks if you use a proxy to connect to Control Manager.
6. At the `Do you access Control Manager through a proxy server? (y/n) [n]` prompt, enter **y** if you do or just press **ENTER** to accept the default choice of **n**. If you choose **n**, the installer asks you to specify the display name to identify ServerProtect on the Control Manager Web console. If you do use a proxy server to connect to Control Manager, see *Entering Proxy Server Information* on page 2-8 for further guidance on this process.
7. At the `Please specify the name you would like to display on the Control Manager console: [SPLX server IP address]` prompt, enter the desired name. Control Manager will use this name to identify your ServerProtect server on the Control Manager Web console. The installer stores this information and asks for the folder in which you would like to present your ServerProtect server on the Control Manager Web console.
8. At the `Please specify a folder name for this product (for example: /SPLX) [New entity]:` prompt, enter the folder path described above. The installer displays a summary of the information you have entered and asks you to confirm your choices.
9. At the `Is the above information correct? (y/n) [n]` prompt, confirm or reject the displayed choices. If you enter **n** (or just press **ENTER** to accept the default choice of **n**), the installer prompts you to re-enter all of the above information, starting with the IP of your ServerProtect server. If you enter **y** to confirm all of the displayed information, an "installation complete" message displays and ServerProtect asks if you would like to enter your activation code. See *Activating ServerProtect During Installation* on page 2-9 for further guidance on this process.

Entering Proxy Server Information

If you use a proxy server to connect to Trend Micro Control Manager, enter your proxy server information during installation so that ServerProtect can communicate properly with Control Manager.

To specify proxy server information during installation:

Enter the following information at the corresponding prompts:

- Proxy Server IP:
- Proxy Server port: [80]
- Does your proxy server require user authentication? (y/n) [n]

  (If authentication is required—)

  - Proxy user name:
  - Proxy password:
  - Confirm proxy password:

The installer stores the information you enter for use with Control Manager and then prompts you to specify the display name to identify ServerProtect on the Control Manager Web console. (See *Setting Up ServerProtect for Use with Control Manager*, Step 6, above.)

Activating ServerProtect During Installation

1. After the installer completes the installation of ServerProtect, it prompts you to register the software. You can do so at this point or skip this step and register later.

```
Step 1. Register
Use the Registration Key that came with your product to register
online
(https://olr.trendmicro.com/registration).
(Please skip this step if the product is already registered.)
```

FIGURE 2-3. Prompts to register ServerProtect during installation

   a. To register now, visit the following URL:

      `https://olr.trendmicro.com/registration`

   b. Follow the steps described in *Registering ServerProtect* starting on page 2-23.

2. The installer prompts you to activate ServerProtect. You can do so at this time or skip this step and activate later. To skip this step, press **Ctrl+D**.

```
Step 2. Activate
Type the Activation Code/serial number received after registration
to activate ServerProtect.
(Press [Ctrl+D] to abort activation.)

Activation Code/serial number: XXXX-XXXX-XXXX-XXXX-XXXX

ServerProtect for Linux has been activated.
```

FIGURE 2-4. Prompts to activate ServerProtect during installation

3. The installation setup program is now complete. If you did not register or activate during installation, you can do so later using methods described in this chapter. See *Registering ServerProtect* on page 2-23 and *Activating ServerProtect* starting on page 2-28 for instructions.

Installing Remotely

Trend Micro understands that many ServerProtect customers install and administer ServerProtect in a centrally managed, distributed environment. For this reason we have provided a remote installation tool (RemoteInstall).

RemoteInstall Features

The RemoteInstall tool has the following features:

- Can install ServerProtect on remote machines
- Configuration file keeps account information of client machines
- Can deploy ServerProtect configuration data to target machines after product installation
- Can deploy Kernel Hook Module (KHM) to target machines after product installation
- Can collect certain information about client environments, such as the running Linux distribution and the Linux kernel number
- Can export configuration information to .CSV format so that in a subsequent deployment RemoteInstall can re-use the list of machines to which the initial deployment failed

The following discussion offers guidelines on—

- Extracting the remote install tool from the ServerProtect binary file
- Using the available options of the remote install tool
- Running the remote install tool
  - Using a configuration file in your deployment
  - Deploying the kernel hook module
  - Assigning clients to deploy to

Extracting RemoteInstall From the ServerProtect Binary

You can use the **`-r`** parameter to extract RemoteInstall from a single package or from the binary file for a specific platform. For example, the following command extracts the remote install tool from the ServerProtect for Linux 2.5 binary file:

```
sh SProtectLinux-2.5.i686.bin -r
```

After you have accepted the license agreement and have extracted the remote installation program (RemoteInstall), the above command creates a `remote.install.splx` subdirectory in your working directory. See Table 2-1,

"RemoteInstall tool directories and files upon extraction," on page 2-12 for a list of files and directories that this subdirectory contains.

File or Directory	*Description*
config/	Directory for ServerProtect configuration file deployment. Contains four files: • `tmsplx.xml` - A ServerProtect config file. User can modify it for deployment. • `tmsplx.xml.template` - A template file for the above config file (`tmsplx.xml`). If `tmsplx.xml` becomes corrupted, user can use this template to restore it. • `xmldeployer` - A script for configuration file deployment. • `xmlvalidator` - A script for validating values of all keys in `tmsplx.xml`
KHM.module/	Directory for KHM file deployment
RemoteInstall	The remote install script itself
RemoteInstall.conf	Configuration file for deployment
RemoteInstall.csv	Template for converting files in `.CSV` format to `.conf` format

TABLE 2-1. RemoteInstall tool directories and files upon extraction

Options Available for Use With the RemoteInstall Tool

Use the **-h** parameter to display the usage of the RemoteInstall parameters:

```
./RemoteInstall -h
```

Parameter	*Description*
-c	check client info
-f {alternative_config_file}	specified config file of remote install. Use this option to run RemoteInstall with a config file other than `RemoteInstall.conf`. (You can use an alternative config file as long as the alternative file contains the same key-value pairs as `RemoteInstall.conf`. See *Using a Configuration File in Your Remote Deployment on page 2-14*)
-h	show usage
-n	do not show license agreement
-p {csv_file}	convert specified csv file to config file for use with RemoteInstall (see *Converting CSV-Formatted Files to RemoteInstall.conf Format on page 2-15* for detailed guidance on this option)
-v	show version

TABLE 2-2. Parameters available for use with RemoteInstall script

Running the RemoteInstall Tool

Follow the major steps outlined below to execute the RemoteInstall program.

To execute RemoteInstall:

1. Place the ServerProtect full binary file on the deploying server.
2. Extract RemoteInstall from the ServerProtect binary. (See *Extracting RemoteInstall From the ServerProtect Binary* on page 2-11 for details.)

3. To deploy ServerProtect to many machines, configure the `RemoteInstall.conf` file for deployment. (See *Running the RemoteInstall Tool* on page 2-13 for detailed guidance on the `RemoteInstall.conf` file.)
4. Issue the following command at the command line:
   `# ./RemoteInstall.`
   RemoteInstall deploys ServerProtect to the target machine(s) and outputs progress messages. The deployment creates the five results files described in Table 2-3, "Results files produced by RemoteInstall script," on page 2-14 below.

Results File	***Description***
splx_failed_list_yyyy-mm-dd_hhmmss.conf	failed list for conf file format
splx_failed_list_yyyy-mm-dd_hhmmss.csv	failed list for `.CSV` file format
splx_success_list_yyyy-mm-dd_hhmmss.conf	success list for conf file format
splx_success_list_yyyy-mm-dd_hhmmss.csv	success list for `.CSV` file format
splx_remote_status_yyyy-mm-dd_hhmmss.txt	deployment status

TABLE 2-3. Results files produced by RemoteInstall script

Using a Configuration File in Your Remote Deployment

The default configuration file used with RemoteInstall is `RemoteInstall.conf`. Upon extraction, this file resides in the ***remote.install.splx*** directory. `RemoteInstall.conf` is a complex configuration file with many keys. You can use this configuration file in three kinds of deployment:

1. ServerProtect 2.5 package deployment and installation
2. ServerProtect 2.5 configuration update
3. Kernel Hook Module (KHM) deployment

For brevity, only the most important configurable keys are listed in the table below. For detailed explanations of every key, please see *Using RemoteInstall.conf* starting on page A-28.

Key	*Description*
DeployOption	Indicates which kind of deployment you want to do. Value 1: ServerProtect 2.5 package deployment and installation Value 2: ServerProtect 2.5 config file update Value 3: KHM deployment
PackageName	Indicates the ServerProtect installation path for package deployment.
Activation Code/serial number	Used in package deployment. Value is the ServerProtect 2.5 Activation Code/serial number for installation.
ConfigFilePath	Used in configuration file deployment. Indicates configuration file path.

TABLE 2-4. Most frequently used configurable RemoteInstall.conf keys

Converting CSV-Formatted Files to RemoteInstall.conf Format

In order to make it easier to modify config files, RemoteInstall provides an option to import files in CSV format. If you would prefer to modify the information in the conf files in a spreadsheet program (such as the one in OpenOffice), follow the procedure below.

To edit and use RemoteInstall conf file in csv format:

1. Import the file `RemoteInstall.csv` into your spreadsheet program, edit it there, and save it with a name other than "RemoteInstall.csv."
2. Copy the new file to your ServerProtect `remote.install.splx` directory.
3. When you run RemoteInstall, use the **`-p`** option followed by the name of the revised `CSV` file, for example:

```
# ./RemoteInstall -p my_conf_file.csv
```

RemoteInstall converts your `CSV` file into `RemoteInstall.conf` format, using the following naming pattern:

```
RemoteInstall_yyyy-mm-dd_hhmmss.conf
```

Remotely Deploying a Kernel Hook Module

When users upgrade the Linux kernel, they need to copy the KHM to the ServerProtect installed directory. IT administrators can use RemoteInstall to deploy the KHM to many machines. Follow the procedure below to remotely deploy a KHM to multiple machines.

To deploy a KHM using RemoteInstall:

1. Download the latest KHM from the Trend Micro kernel support Web site (`http://www.trendmicro.com/en/products/file-server/sp-linux/use/kernel.htm`).
2. Copy the KHM to its corresponding directory on the deploying server.
3. Run RemoteInstall.

Tip: Trend Micro recommends testing the deployment on a small number of machines before executing a deployment to your entire network.

Targeting Clients for Remote Deployment

Revise the information in the *Client assignment* section of `RemoteInstall.conf` to target clients for remote deployment. Under this section are two subsections for use in targeting remote computers. Edit the first section, (***`#single deploy`***), to input the configuration for a single machine to which RemoteInstall will deploy. Edit the second section, (***`#group deploy`***) to input configurations for one or more groups of clients. You can use both sections in a single deployment.

The discussion below lists the configuration data that you need to input for a successful deployment.

Single Deploy

In the ***#single deploy*** subsection of the *Client assignment* section of `RemoteInstall.conf` are 13 configuration items that RemoteInstall must be aware of in order to deploy successfully

Line	*Description*
1. [x.x.x.x]	IP address of client
2. RootPassword	root password of client
3. ConnectCM	Value 1 (the default): register to Trend Micro Control Manager (TMCM) server. Value 0: do not register to TMCM sever
4. CMServerIP	IP address of TMCM server
5. CMServerPort	connection port of TMCM server (default = 80)
6. UseProxyAccessCM	Value 1: use a proxy server to connect to TMCM server. Value 0 (the default): do not use proxy
7. ProxyServerIP	IP address of proxy server
8. ProxyServerPort	connection port of proxy server (default = 80)
9. ProxyAuthentication	Value 1: use proxy authentication Value 0 (default): do not use
10. ProxyUserName	Proxy authentication user name
11. ProxyPassword	Proxy authentication password
12. CMClientName	Client machine name that displays in TMCM console. Default = IP address of client
13. CMProductDirectoryName	Directory name that displays in TMCM console. Directory is used to group clients. Default = “New entity”

TABLE 2-5. Client assignment keys in configuration file, single deploy

Group deploy

For group deployment, all of the lines are identical to those in the ***#single deploy*** section except for the following.

Line	*Description*
1. [Group1]	Instead of a key for the IP address of a single machine, the first key labels the group of clients to deploy to.
14. Machine1=x.x.x.x	In this line (and as many as needed after it), list the IP address of each machine to which RemoteInstall will deploy ServerProtect.
15. Machine2=x.x.x.x	(same as above)
(list as many as needed)	(same as above)

TABLE 2-6. Client assignment keys in configuration file, group deploy

Tip: For ease of reference, Trend Micro suggests starting any group names with an easily identifiable term, such as *Group1, Group2, Group3,* and likewise for machine names, for example, *Machine1, Machine2,* and so on.

Logging On to the ServerProtect Web Console

To open the Web console, type one of the following in the URL address field in a browser window and press **ENTER**:

```
http://{host server IP}:14942
https://{host server IP}:14943
```

The Logon screen displays in your browser window. There are two versions of the Logon screen, depending on whether you registered and activated ServerProtect during installation.

If you registered and activated, a fully licensed ("standard") version of the product was installed. If you skipped registration and activation, an evaluation version of the product was installed. The evaluation version is fully functional, but when the 60-day evaluation period ends, you will stop receiving new pattern files or scan engine updates from Trend Micro. Updates will not resume until you register and activate ServerProtect.

If you have already registered and activated your copy of ServerProtect, the Logon screen appears as follows:

FIGURE 2-5. ServerProtect Web console Logon screen when ServerProtect is registered/activated

If you have not registered and activated ServerProtect, the Logon screen includes prompts to register ServerProtect using your Activation Code/serial number. The screen appears as follows:

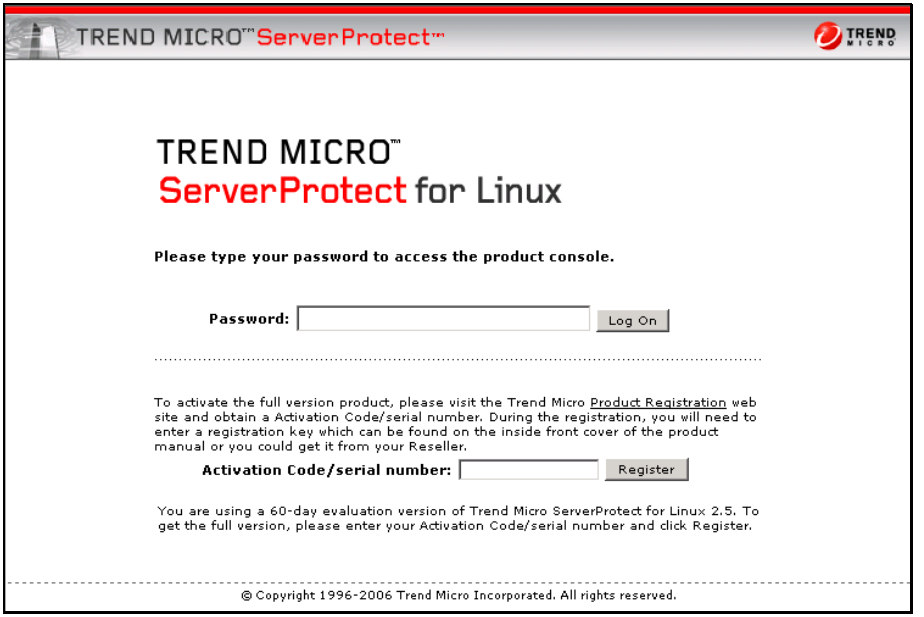


FIGURE 2-6. Logon screen when ServerProtect is not registered/activated

A password is not required to access the application the first time you log on after installing. Click **Log on**. The following screen displays:

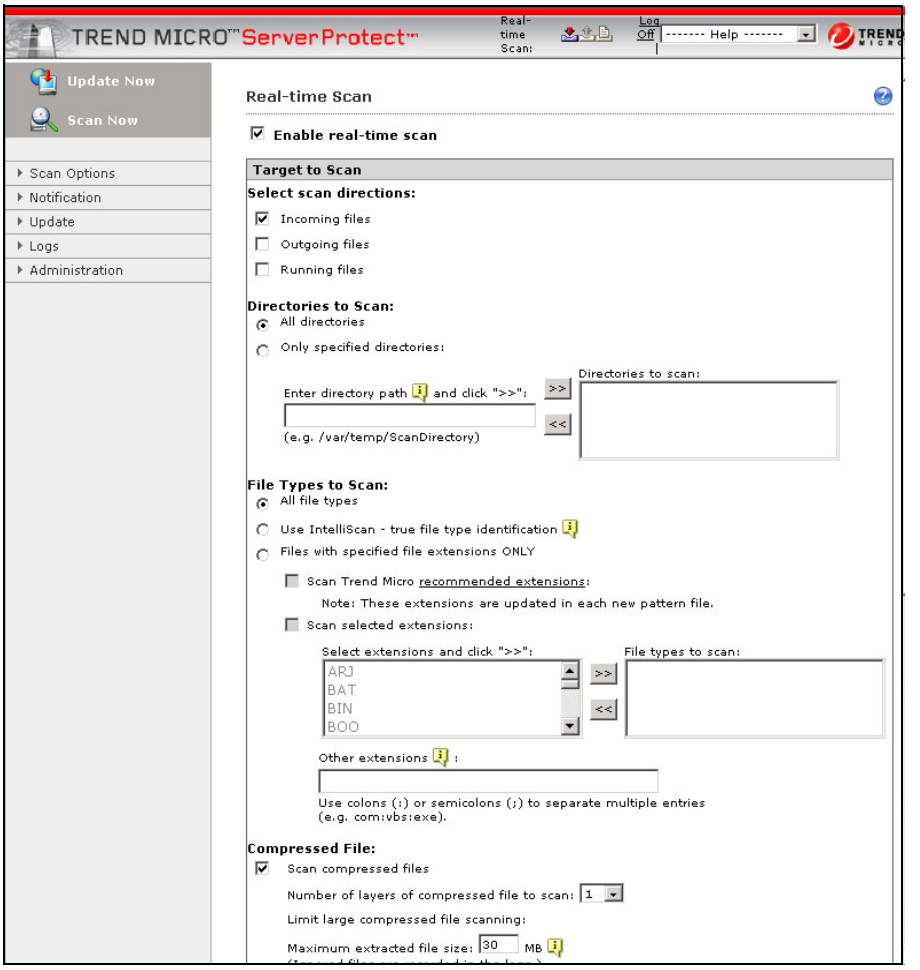


FIGURE 2-7. Default view of the Web console after login

The Real-time Scan screen is the default view when the Web console opens.

Note: Real-time scanning is enabled by default.

Make selections from the left menu to navigate the user interface. For example, your next action should be to set up your administrator account with a password, before you log off from the ServerProtect Web console.

Setting Up an Administrator Password

To navigate to the Password screen, select **Administrator** > **Password**. The Password screen displays. ServerProtect prompts you to supply your current password and your new password and to confirm your new password. During first logon, supply the same information in all three fields. However, you can change your password at a later time on this screen. See *To configure ServerProtect Web console passwords:* on page 3-11 for more information.

Note: When you first log on to the ServerProtect Web console after installation, the password is blank. (There is no default password.)

For information on how to reset the password from the command line, see the description of the `-f` command in *Using splxmain* starting on page A-30.

Registering ServerProtect

Trend Micro provides all registered users with technical support, virus pattern downloads, and program updates for 1 year, after which you must purchase renewal maintenance to continue receiving these services. Register ServerProtect to ensure that you are eligible to receive the latest security updates and other product and maintenance services. You can register ServerProtect during or after installation.

When you purchase ServerProtect, you will receive a Registration Key or serial number (also referred to as an Activation Code) from Trend Micro or your reseller.

Registration Key Format

A Registration Key uses 22 characters, including hyphens, and displays in the following format:

```
XX-XXXX-XXXX-XXXX-XXXX
```

Serial Number (Activation Code) Format

A serial number (also referred to as an Activation Code) uses 24 characters, including hyphens, and displays in the following format:

```
XXXX-XXXX-XXXX-XXXX-XXXX
```

Note: Some resellers may register ServerProtect for you and give you your serial number directly.

To register your software using your Registration Key:

1. First, verify that you have received a Registration Key for ServerProtect. If you have not, contact your reseller.
2. On the ServerProtect Web console, click **Administration** > **Customer Registration** on the left menu. The Customer Registration screen displays.
3. Click the Trend Micro Product Registration Web site link. The Online Registration page of the Trend Micro Web site opens in a secondary browser window.

4. In the Enterprise/SMB User section of the Online Registration page, click the Click here (to register your product) link. The following screen displays.

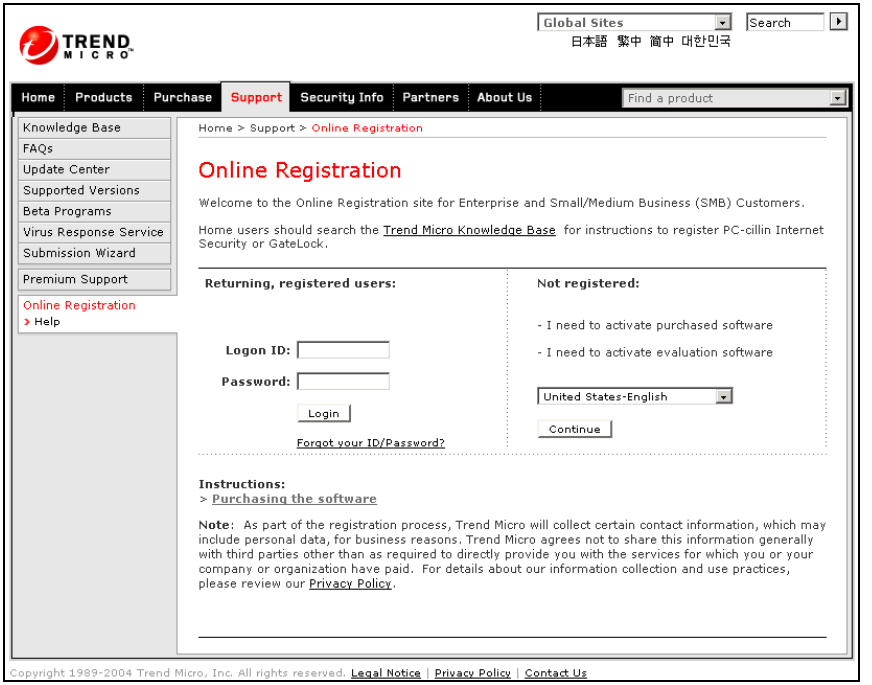


FIGURE 2-8. The Trend Micro Online Registration Web site

5. If you are an existing customer and you already have a customer logon ID and password, enter your logon ID and password on the left side of the screen and click **Login**. If you are not a registered user, click **Continue** on the right side of the screen.
6. On the Enter Registration Key page, type or copy the ServerProtect **Registration Key**, and click **Continue**.
7. On the Confirm License Terms page, read the license agreement and then click **I accept** to agree to the terms of the license agreement.
8. On the Confirm Product Information page, click **Continue Registration**.

9. Follow the prompts to complete the online registration form, and then click **Submit**.
10. Click **OK** twice. After the registration is complete, Trend Micro sends you a serial number (also referred to as an Activation Code) by email, typically within 20 minutes. You can activate ServerProtect using that number.

If you already have a ServerProtect 2.5 serial number (also referred to as an Activation Code), follow the procedure below to register your ServerProtect software.

To register your software using an Activation Code/serial number:

1. On the Web console, click **Administration** > **Product Registration** on the left menu. The Product Registration screen displays.
2. Type your serial number in the **Activation Code/serial number** field and click **Register**. You do not have to include the hyphens when typing your serial number.

If you use a proxy server to access the Internet, follow the procedure below to configure your proxy settings.

To configure proxy settings:

1. Click **Update > Proxy Settings**. The Proxy Settings screen displays:

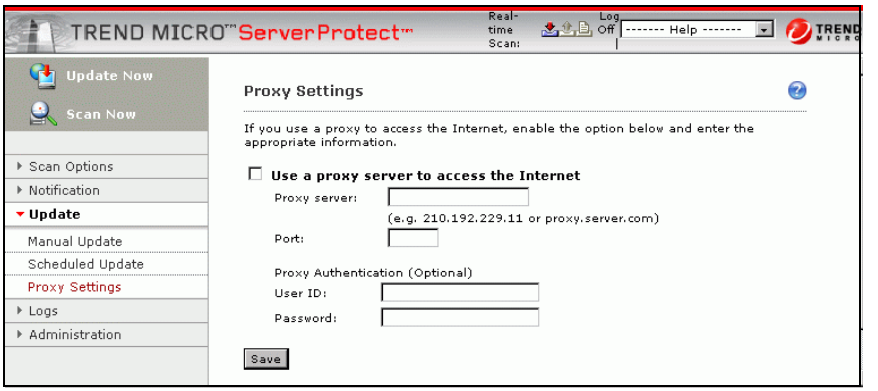


FIGURE 2-9. Proxy Settings screen

2. Select the **Use a proxy server to access the Internet** checkbox.
3. In the **Proxy server** field, type the IP address or host name of the proxy server.
4. In the **Port** field, type the proxy server listening port number.
5. If you are using an optional proxy authentication user ID and password, type this information in the **User ID** and **Password** fields.
6. Click **Save**.

Tip: Trend Micro recommends that you update the virus pattern file and scan engine immediately after installation. If you use a proxy server to access the Internet, configure your proxy server settings first, before updating the scan engine and pattern file.

To update components:

1. Click **Update > Manual Update**. The Manual Update page displays.

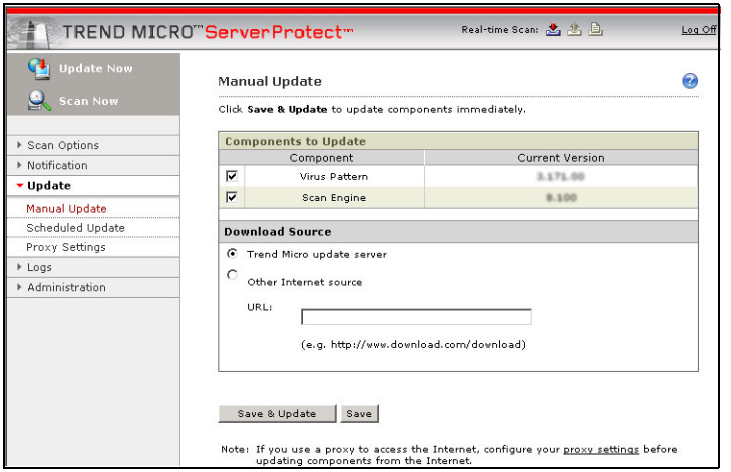


FIGURE 2-10. Manual Update screen

2. Select the **Virus Pattern** and **Scan Engine** check boxes.
3. Click **Save & Update**.

Activating ServerProtect

Use your Registration Key to register ServerProtect and obtain a serial number (also known as an Activation Code) from the Trend Micro Online Registration Web site to install a standard (not evaluation) version. The Web site is:

`https://olr.trendmicro.com/registration/us/en-us/login.aspx`

After completing the registration, Trend Micro issues a serial number (Activation Code) that you use to activate Trend Micro software and other Trend Micro services.

Trend Micro recommends that you activate ServerProtect during installation. However, if you have installed ServerProtect without activating it, you can still activate it afterwards.

After installation, you can activate ServerProtect in three different ways.

To activate ServerProtect at the Logon screen:

1. Type the product serial number (Activation Code) in the **Activation Code/serial number** field.
2. Click **Register.** ServerProtect activates.

To activate ServerProtect at the Product Registration screen:

1. On the ServerProtect Web console, select **Administration** > **Product Registration** from the left menu.
2. Type the product serial number (Activation Code) in the **Activation Code/serial number** field.
3. Click **Register.** ServerProtect activates.

To activate ServerProtect at the command prompt:

1. Navigate to the following directory:

   `/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp`

2. Issue the following command:

   `splxmain -q <Activation Code/serial number>`

   ServerProtect activates.

Converting an Evaluation Version to Standard

If you typed **Ctrl+D** at the registration/activation step during installation, the setup program installs a 60-day evaluation version of the product. You can view the status of your installed product (either an evaluation version or standard version) on the Product Registration screen. In the following example, an evaluation version is installed.

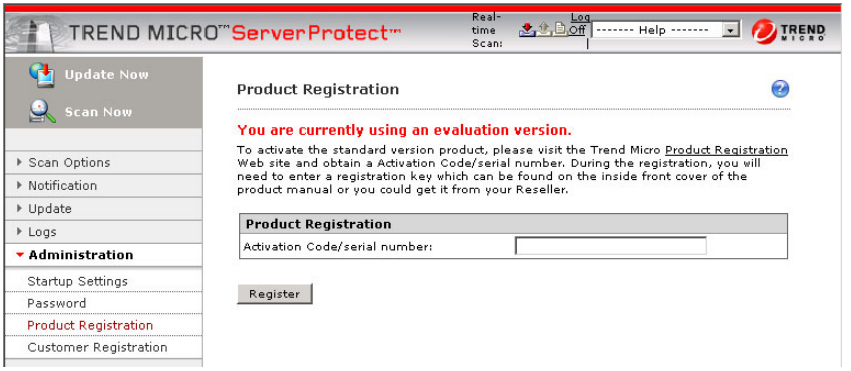


FIGURE 2-11. Product Registration screen for a user with an evaluation version of ServerProtect

To continue using ServerProtect after the evaluation period, register and activate the product. Use the Registration Key included in the ServerProtect package or purchase one from your Trend Micro reseller to obtain a serial number (also referred to as an Activation Code) from Trend Micro Online Registration as described in *Activating ServerProtect* starting on page 2-28.

Verifying the Installation

After completing the installation, verify that ServerProtect is running optimally.

To verify that ServerProtect is running optimally:

1. Type the following at the command line:

   ```
   /etc/init.d/splx status
   ```

2. The output should show all running processes, for example:

   ```
   splxmod module is running...
   vsapiapp (pid 3854) is running...
   entity (pid 3845 3844) is running...
   ServerProtect for Linux core is running...
   splxhttpd (pid 3869 3868 3867 3866 3865 3864) is running...
   ServerProtect for Linux httpd is running...
   ServerProtect for Linux manual scan is stopped
   ServerProtect for Linux scheduled scan is stopped
   ServerProtect for Linux Control Manager agent is not registered
   to Trend Micro Control Manager server
   ```

Removing ServerProtect

In order to remove ServerProtect, you must be logged on as *root.* The uninstallation commands are different depending on which Linux distribution your system is using, as shown in the table below. Both commands shown stop the ServerProtect service and remove the application.

Linux Distribution	Uninstall Command
Red Hat	`rpm -e SProtectLinux`
SUSE	
Novell Desktop Linux 9	
Debian	`dpkg --purge sprotectlinux`

TABLE 2-7. Commands to remove ServerProtect for Linux, by Linux distribution

Installing a Kernel Hook Module

Real-time scanning is disabled if you do not have the appropriate kernel hook module installed for your operating system. This section describes how to install the kernel hook module (KHM) for your server if you are not using the default kernels provided during installation of ServerProtect for Linux or if the KHM is updated after installation and you need to install a more current version of the KHM.

To install an alternate kernel hook module:

1. Log on as *root*.
2. To verify that your kernel is supported by the latest version of ServerProtect, visit the following URL:

   `http://www.trendmicro.com/en/products/file-server/sp-linux/evaluate/overview.htm`

   KHMs are named after their corresponding kernel version.
3. Download the relevant KHM package and copy the KHM package to the following directory:

   `/opt/TrendMicro/SProtectLinux/SPLX.module/`

4. Go to the directory mentioned in step three, and then extract the KHM files using the following command:

   `tar xzvf {SPLX version and kernel version}.tar.gz`

   The following files are extracted from the package:

   - {kernel version}.md5
   - splxmod-{kernel version}smp.o for symmetric multi-processors
   - splxmod-{kernel version}.o for uni-processor

Tip: Trend Micro strongly recommends that you verify the MD5 checksum of ServerProtect kernel hook modules to make sure the files have been downloaded and extracted intact.

---

5. Start the ServerProtect service by issuing the following command:

   ```
   /etc/init.d/splx start
   ```

6. After installation, you can access the ServerProtect Web console at:

   ```
   http://<host server>:14942/
   ```

7. Make sure your Linux system port 14942 is already open for ServerProtect access.

Chapter 3

Getting Started with ServerProtect

This chapter helps you start using ServerProtect. It provides basic setup and usage instructions. Additional information is available by searching these topics in the online help.

This chapter discusses the following topics:

Testing ServerProtect Installation

The European Institute of Computer Antivirus Research (EICAR), in cooperation with antivirus vendors, has developed a test file to verify whether your system detects viruses.

The file is not an actual virus; it will cause no harm and it will not replicate. Rather, it is a specially created file whose "signature" has been included in the Trend Micro virus pattern. As a result, the Trend Micro scan engine will detect it.

You can download the EICAR test file from the Trend Micro Web site at:

`http://www.trendmicro.com/vinfo/testfiles/index.htm`

You may need to disable HTTP scanning, if any, before downloading the file. Include the test file as an email attachment to test SMTP scanning, and to check FTP and HTTP file transfers, for example, if you have Trend Micro InterScan VirusWall™ installed on the network.

Alternatively, copy the following characters into a text file, and then save the file with a `com` extension (for example, `virus.com`):

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

For either option, the mere downloading or creation of the file should be enough to trigger real-time scanning.

Accessing ServerProtect Using the Quick Access Console Menus

When you have KDE 3.2 or 3.3 installed on the server hosting ServerProtect, the ServerProtect installation program adds the TrendMicro ServerProtect Administration menu option to your desktop in the following places:

- System Tools Menu (Red Hat platforms)
- System Menu (SUSE and Debian platforms)

Note: Accessing the Quick Access console requires logging on as a *root* user. The default setting of XWindows on the Debian platform does not support root login.

For example:

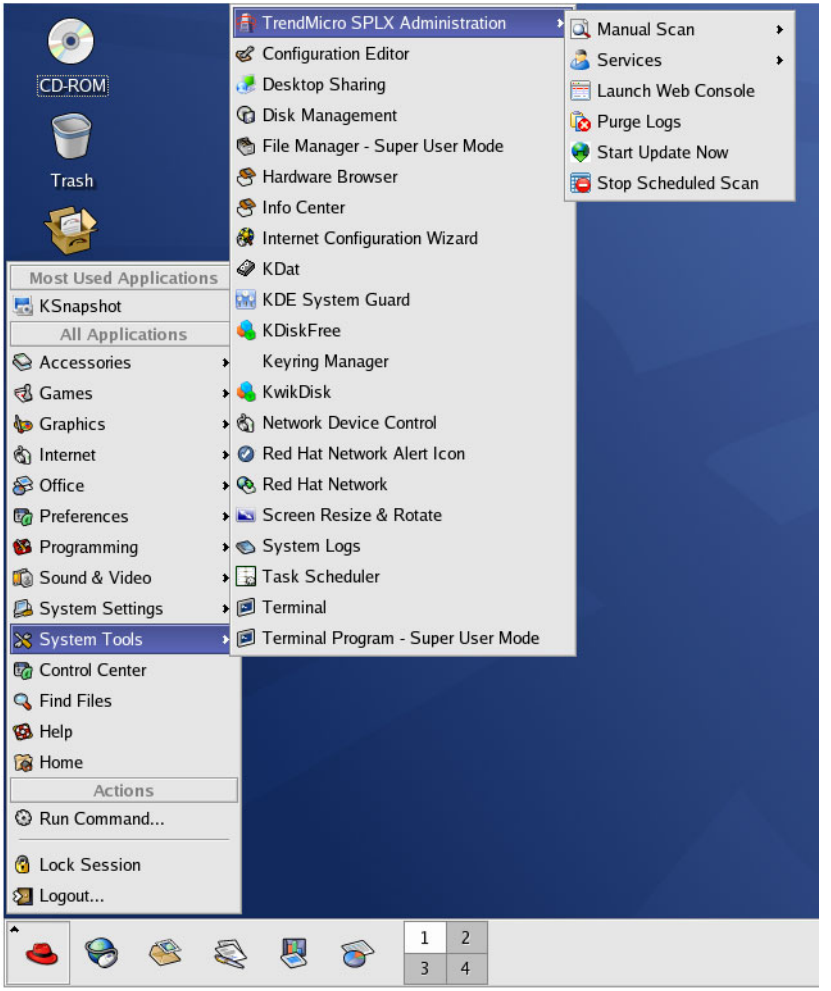


FIGURE 3-1. TrendMicro ServerProtect Administration menu option added to the KDE desktop

The following menus/options are available on the TrendMicro ServerProtect Administration menu:

- **Manual Scan menu**—This menu allows you to start or stop manual scanning

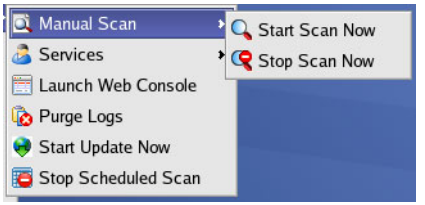


FIGURE 3-2. Manual Scan menu

- **Services menu**—This menu allows you to start or stop ServerProtect service, and starting or stopping Apache Web server (Httpd) service

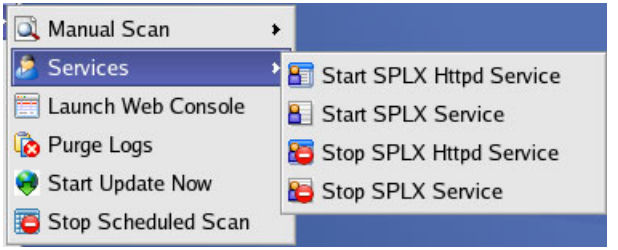


FIGURE 3-3. Services menu

- **Launch Web Console**—This menu option allows you to launch the Web console from your desktop, instead of typing the Web console URL in your browser
- **Purge Logs**—This option purges all scan, virus, and system logs
- **Start Update Now**—This option starts a download of the most recent virus pattern file and scan engine from your update server
- **Stop Scheduled Scan**—This option stops an ongoing scheduled scan

Starting and Stopping ServerProtect

You can start ServerProtect from either the command line, or the XWindow Quick Access console.

Note: By default, ServerProtect starts whenever you turn on the server hosting it. To change this setting, see *Configuring Start-Up Settings on page 3-7.*

Starting ServerProtect

There are two ways to start ServerProtect:

- From the command line
- From the XWindow Quick Access console

To start ServerProtect from the command line:

1. Log on as *root*.
2. Type the following at the command line: `/etc/init.d/splx start`

   The following messages appear.

```
Starting ServerProtect for Linux:
Checking configuration file:                    [OK]
Starting splxcore:
Loading splx kernel module:                     [OK]
Starting vsapiapp:                              [OK]
Starting Entity:                                [OK]
ServerProtect for Linux core started.
                                                [OK]
Starting splxhttpd:
Starting splxhttpd:                             [OK]
ServerProtect for Linux httpd started.
                                                [OK]
ServerProtect for Linux started.
linux:~#
```

To start ServerProtect from the Quick Access console:

1. Log on as *root*.
2. From the task bar on the XWindow main window (KDE 3.2 or higher), click **Start Applications Menu** > **System (Tools)** > **TrendMicro SPLX Administration** > **Services** > **Start SPLX Service**.

Note: On Red Hat platforms, the file path is **Start Applications Menu > System Tools > TrendMicro SPLX Administration > Services > Start SPLX Service**. On all other platforms, the word "Tools" is not displayed after the word "System." The notation used in this document is **Start Applications Menu > System (Tools) >** and so on.

Stopping ServerProtect

There are two ways to stop ServerProtect:

- From the command line
- From the XWindow Quick Access console

To stop ServerProtect from the command line:

1. Log on as *root*.
2. Type the following: `/etc/init.d/splx stop`

   The following messages appear.

```
Shutting down ServerProtect for Linux:
Shutting down splxcore:
Shutting down vsapiapp:                                    [OK]
Unloading splx kernel module:                              [OK]
Shutting down entity:                                      [OK]
ServerProtect for Linux core stopped normally.
                                                           [OK]
Shutting down splxhttpd:
Shutting down splxhttpd:                                   [OK]
ServerProtect for Linux httpd stopped normally.            [OK]
ServerProtect for Linux stopped normally.                  [OK]
linux:~#
```

To stop ServerProtect from the Quick Access console:

1. Log on as *root*.
2. From the task bar on the XWindow main window (KDE 3.2 or higher), click **Start Applications Menu** > **System (Tools)** > **TrendMicro SPLX Administration** > **Services** > **Stop SPLX Service**.

Configuring Start-Up Settings

By default, ServerProtect for Linux starts whenever you turn on the server hosting it. To change this setting, use the Linux Setup utility.

The method of configuring startup settings varies for each Linux distribution supported by this release. For instructions on configuring start-up settings for your Linux distribution, see the applicable section below:

Red Hat™ Enterprise Linux 4:

Using the GUI:

a. Log on as *root* and type `system-config-services` from the command line. The Setup Utility UI appears.

b. Select **Edit Runlevel** on the menu and then choose level 3 to 5 to edit.

c. Select **splx** and mark the appropriate run levels.

d. To start the service manually, unmark **splx** on level 3 to 5.

Using the terminal only:

a. Log on as *root* and type `setup` from the command line. The Setup Utility UI appears.

b. Find and select **System services.**

c. Select **splx** to configure ServerProtect to start automatically. Deselect **splx** to start manually.

SUSE Linux Enterprise Server 9 and Novell™ Linux Desktop 9:

Using the GUI only:

a. Log on as *root* and type `yast2` from the command line. The Setup Utility UI appears.

b. Select **System** > **Runlevel Editor** on the menu.

c. Select **Expert Mode** > **splx** and mark the appropriate run levels.

d. To start the service automatically, choose level 3 or 5. To start the service manually, do not select a level.

Using the terminal only:

a. Log on as *root* and type `yast` from the command line. The Setup Utility UI appears.

b. Select **System** > **Runlevel Editor** on the menu and press Enter.

c. Select **Expert Mode** > **splx** and mark the appropriate run levels.

d. To start the service automatically, choose level 3 or 5. To start the service manually, do not select a level.

Debian (terminal interface only):

1. Log on as *root* and type `rcconf` from the command line.
2. Select **splx** to start the service automatically. Deselect **splx** to start the service manually.

For help with these startup settings in the ServerProtect Web console, select **Administration > Startup Settings** and click the system administration tool link. The following screen appears:

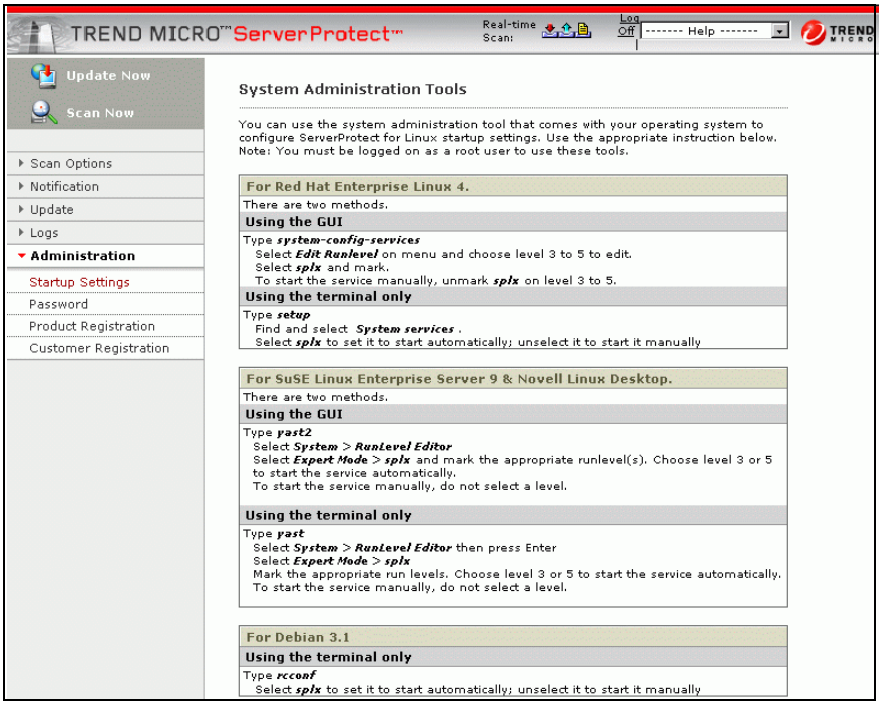


FIGURE 3-4. System Administration Tools screen

Using the ServerProtect Web Console

This section describes how to use the Web-based console to configure ServerProtect. The console permits local and remote as well as multiple-user control of the application via a browser. See *Supported XWindow Graphical Desktop Environments* on page 2-3 to check which browsers are compatible with ServerProtect.

Note: Trend Micro recommends using only one Web console at a time for configuring ServerProtect. Otherwise, changes made by one user will be overwritten by another user accessing the same Web console option.

Access the Web console through the XWindow Quick Access console, or directly through a browser.

To access the Web console:

1. Log on as *root*.
2. Do one of the following:
   - From the task bar on the XWindow main window (KDE 3.2 or 3.3), click **Start Applications Menu** > **System (Tools) > TrendMicro SPLX Administration > Launch Web Console**.
   - Type the location of the ServerProtect host and the static port used for the console in the browser's address field. For example:

     `http://<host name>:14942/`

     `https://<host name>:14943/`

     The `<host name>` is either the computer host name or its IP address.

     14942 is the default HTTP port number used by ServerProtect.

     14943 is the default HTTPS port number used by ServerProtect.

     Note: To change the port numbers, use `splxmain`. See *Using splxmain* starting on page A-30 for more information.

     ---

3. Type the Web console password, then press **Enter**. By default, the password field is empty (that is, there is no default password).

Tip: For protection, change the Web console password after logging in for the first time. To learn how to change the Web console password, see *To configure ServerProtect Web console passwords:* on page 3-11.

To log off from the Web console:

To log off from the console, simply click  on the title bar.

Things to Remember About the ServerProtect Web Console

- The Web console provides access to all ServerProtect functions. However, it cannot start or stop the application. To do this, use the command line or the Quick Access console. See *Accessing ServerProtect Using the Quick Access Console Menus* on page 3-2.
- The Web console automatically refreshes every hour. Refresh it manually using your browser's Refresh option.

To configure ServerProtect Web console passwords:

1. Select **Administration** > **Password** from the left menu on the Web console.
2. Type the current password in the **Current password** field.
3. Type the new password in the **New password** field. Passwords must not exceed 32 characters, and should contain alphanumeric characters (A-Z, a-z, 0-9) and hyphens (-).
4. Re-type the password for confirmation.
5. Click **Save**.

Note: Always protect your Web console password. Trend Micro recommends that you set your password immediately after installation.

Updating the Scan Engine and the Virus Pattern File

ServerProtect ships with scan engine and pattern files that are current at the time of release of the product. The most recent threats may not be addressed by these components, so Trend Micro recommends that you update them immediately after installing ServerProtect. Updating the following files using ActiveUpdate, the Trend Micro Internet-based component update feature:

- *Virus Pattern File* - This file contains thousands of malware signatures (for example, viruses, Trojans, and so on), and determines ServerProtect's ability to detect these hazardous files. Trend Micro updates pattern files at least once a week to ensure protection against the latest threats.
- *Scan Engine* - This component performs the actual scanning and cleaning functions. The scan engine employs pattern-matching technology, using signatures in the pattern file to detect viruses, Trojans, and malicious programs. Trend Micro occasionally issues a new scan engine to incorporate new technology.

You can perform updates manually, or let ServerProtect perform them according to a schedule. Trend Micro recommends performing a manual update immediately after installation. Only registered users are eligible for scan engine and virus pattern updates; see *Registering ServerProtect* starting on page 2-23 for more information.

Note: If your company uses a proxy to access the Internet, configure ServerProtect's proxy settings before attempting an update.

To configure proxy settings:

1. Select **Update** > **Proxy Settings** from the left menu.
2. Enable **Use a proxy server to access the Internet**.

3. Provide the following information as required:
   - **Proxy server** - specify the proxy server's address in IP address or DNS format, for example, `123.123.123.123` or `splxproxy.trendmicro.com`
   - **Port** - specify the port number used by the proxy server

   If your proxy requires authentication, supply the following:
   - User ID
   - Password

Note: To set the proxy password from the command prompt, refer to *Using splxmain* on page A-30.

Configuring a Manual Update

ServerProtect allows you to perform updates on-demand (Update Now). This is a particularly useful feature during virus outbreaks (when updates do not arrive according to a definite schedule), and when using ServerProtect for the first time.

There are two ways to perform an Update Now, either by using existing settings, or after configuring new settings.

To use the saved settings do one of the following:

- Click 

on the left menu.
- From the task bar on the XWindow main window, click **Start Applications Menu** > **System (Tools)** > **TrendMicro SPLX Administration** > **Manual Update** > **Start Update Now**.

To update after configuring update settings:

1. Select **Update** > **Manual Update** on the left menu. The Manual Update screen appears.
2. Select the check box of the update component. The current version of each component appears to the right of the component label. For example:

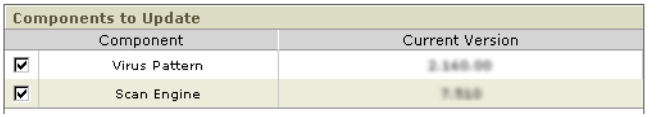


FIGURE 3-5. Components to Update section of the Manual Update screen

3. Next, select a download source, as explained in *Specifying a Download Source* starting on page 3-14.

FIGURE 3-6. Download Source section of the Manual Update screen

4. Click **Save & Update**.

Specifying a Download Source

Depending on whether or not ServerProtect is being managed by Trend Micro Control Manager (TMCM), the download source differs, because only manual update is available when ServerProtect is not working in conjunction with TMCM.

Update Behavior When ServerProtect Is Managed by Control Manager

When ServerProtect is being managed by Trend Micro Control Manager, updates come automatically, either through the normal Control Manager update policy or when an Outbreak Prevention Policy has been triggered. The default download source for TMCM updates is:

```
http://xxx.xxx.xxx.xxx/TVCSDownload/ActiveUpdate
```

...where xxx.xxx.xxx.xxx is the Control Manager IP address.

Update Behavior When ServerProtect Is Not Managed by Control Manager

When ServerProtect is not being managed by TMCM, you can update components only via the Update Now (Manual Update) function. The default download source in that case is:

```
http://splx-p.activeupdate.trendmicro.com/activeupdate
```

To customize the download source:

1. Configure manual (see *Configuring a Manual Update* starting on page 3-13) or scheduled update (see *Configuring Scheduled Updates* starting on page 3-16).
2. On the working area, select one of the following download sources:
   - **Trend Micro update server** - the default update server that displays when ServerProtect is not being managed by Control Manager

     —or—

   - **Trend Micro Control Manager update server** - the default update server that displays when ServerProtect is being managed by Control Manager

     ServerProtect implements digital signature checking whenever it downloads components from the ActiveUpdate server.
   - **Other Internet source**—specify HTTP or HTTPS Web site (for example, your local Intranet Web site), including the port number that should be used from where ServerProtect can download updates

     The update components have to be available on the primary update source (Web server). Provide the host name or IP address, and directory (for example, https://12.1.123.123:14943/source). In addition, you can set up multiple backup update servers/sources to automatically fail over in case the primary update source fails.

Note: To use multiple backup update sources, servers running ServerProtect must first successfully complete one update from the new primary update source. If you need assistance setting up the primary update source and additional backup update sources, please contact Trend Micro technical support.

Configuring Scheduled Updates

Scheduled updates allow you to perform regular updates without user interaction; thereby, reducing your workload.

To configure a scheduled update:

1. Select **Update** > **Scheduled Update** on the left menu. The Scheduled Update screen appears.
2. Select the **Enable Scheduled Update** check box.
3. Select the check box of the update components. The options are:
   - Virus pattern
   - Scan engine

   Select a download source, as discussed in *Specifying a Download Source* starting on page 3-14.

   You can set up multiple backup update servers/sources to automatically failover in case the primary update source fails.

   Note: To use multiple backup update sources, servers running ServerProtect must first successfully complete one update from the new primary update source. If you need assistance setting up the primary update source and additional backup update sources, please contact Trend Micro technical support.

4. Configure a download schedule. Select a start time in hours and minutes from the **Start time** menu.

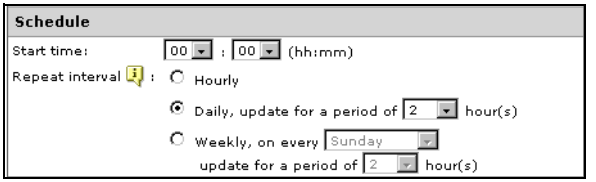


FIGURE 3-7. Schedule section of the Scheduled Update screen

5. Specify a repeat interval. The options are **Hourly**, **Daily**, and **Weekly**. For weekly schedules, specify the day of the week (for example, Sunday, Monday, and so on.)

Note: The **Daily** and **Weekly** fields offer you an interval called **update for a period of *x* hours**. This means that your update will take place sometime within the *x* number of hours specified, following the time selected in the **Start time** field. This feature helps with load balancing on the ActiveUpdate server. Alternatively, you can specify an exact time if you prefer. Hover your cursor over the tooltip icon ( ) for more explanation of this feature, and examples.

---

6. Click **Save**.

Chapter 4

Configuring and Performing Scans with ServerProtect

This chapter discusses the following topics:

Configuring Scanning Options

After installing ServerProtect and updating the virus pattern and scan engine, you can configure the scanning options.

FIGURE 4-1. ServerProtect Web console left menu with Scan Options expanded

Kernel Dependent and Independent Modes

ServerProtect 2.5 comes in two modes:

- Kernel-dependent mode – Aside from manual and scheduled scanning, ServerProtect provides real-time scanning for Linux distributions and kernels supported by the Kernel Hooking Module (KHM) embedded in the installation program. ServerProtect automatically installs the appropriate KHM for supported Linux distributions and kernels.

Note: In kernel-dependent mode, the default initial view of the Web console is the Real-time Scan page.

- Kernel-independent mode – ServerProtect provides manual and scheduled scanning for Linux distributions and kernels that do not support the Kernel Hooking Module embedded in the installation program. In this mode, all real-time scan-related options in the ServerProtect Web console are disabled.

  Note: In kernel-independent mode, the default initial view of the Web console is the Manual Scan page.

ServerProtect, in kernel-dependent mode, can perform three types of scanning: real-time (Real-time Scan), manual (Scan Now), and scheduled. ServerProtect in kernel-independent mode performs manual and scheduled scanning.

The scan types are explained below:

Scan Type	Description
Real-time	This type of scan runs each time a file is accessed or executed. Real-time Scan examines incoming, outgoing, and running files.
Scheduled	Also known as Scheduled Scan, this scan type is similar to a manual scan, except that it follows a specified schedule.
Manual	Also known as Scan Now, this scan type performs a thorough scan of your server upon demand.

TABLE 4-1. ServerProtect scan types, described

Understanding Scanning Options

Real-time scanning is always monitoring the traffic coming in, going out, and/or executing on your servers. Trend Micro recommends that real-time scanning always be enabled.

In addition, the scheduled scan gives you an opportunity to do a periodic look at your servers, perhaps on a weekly basis. The scheduled scan allows you to include directories or file types that you do not constantly monitor using real-time scanning. Because a scheduled scan might be more inclusive, it could utilize more of your computing resources; thus, you might want to arrange scheduled scans for non-peak hours, such as early Sunday morning.

Finally, the manual scan allows you to do a scan of your servers on demand. For example, when an outbreak occurs, there is a period of vulnerability between the time

of discovery and the release of the Trend Micro pattern file designed to detect the new threat. Even though that period is typically a matter of hours, your servers may be vulnerable during that time. After ServerProtect downloads the updated pattern file, run a manual scan to see whether any malware arrived on your servers while you were vulnerable. Another time to perform a manual scan is when the servers are back online after maintenance downtime.

Configure each of the above scan types independently. Configuration options common to all scanning types: virus actions, locations to scan, file types to scan, and compressed file scanning, are discussed below as independent topics.

Note: To find out more about the scanning technologies ServerProtect employs, see to *Protecting Linux Servers* on page 1-2.

Understanding Virus Actions

You can perform a variety of actions on detected viruses, as shown in Table 4-2, “Actions that ServerProtect can take against detected viruses,” on page 4-4 .

Action	Description
Clean	Removes virus code from infected files.
Quarantine	Move infected or malicious files to a restricted access directory.
Rename	Modify the extension of the infected file to prevent any program from opening or executing it. ServerProtect gives renamed files the extension "VIR."
Delete	Remove infected or malicious files.
Pass	Record virus infections or malicious files in the scan logs, but take no action. This choice is not recommended.

TABLE 4-2. Actions that ServerProtect can take against detected viruses

To specify locations to scan:

1. On the left menu, select **Scan Options**, then choose the scan method.
2. Under the **Select directories to scan** section, select the desired scan coverage.

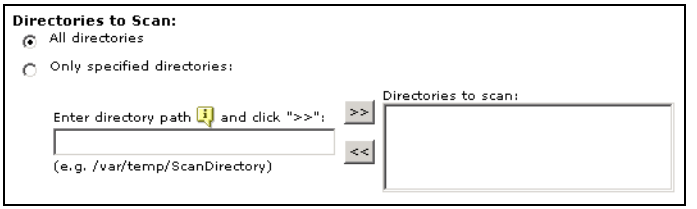


FIGURE 4-2. Select directories to scan

The options are:

- **All directories**—scans all directories, except those included in the Exclusion List. For additional information on the Exclusion List, refer to *What is the Exclusion List?* in the online help.
- **Only specified directories**—limits the scan to the directories and subdirectories that you specify. To do so:

  i. Type the target directory in the **Directory path** field. For example: `/var/temp/ScanDirectory`

  Note that directory path names are case-sensitive.

  ii. Click >> to add the entry to the **Directories to scan** list.

  iii. Add other directories as required.

Note: You can use an asterisk (*) or question mark (?) as a wildcard for entering the directories to be scanned.

To remove directories that you previously specified:

1. Select the directory for removal in the **Directories to scan** list.
2. Click << to remove the selected entry.
3. Click **Save** to apply your settings.

Specifying Files to Scan

Configuring ServerProtect to scan files known to be vulnerable to infection significantly reduces scanning time and therefore conserves system resources.

To specify files to scan:

1. On the left menu, select **Scan Options**, then choose the scan method.
2. Under **Select file type to scan**, click the desired scan coverage.

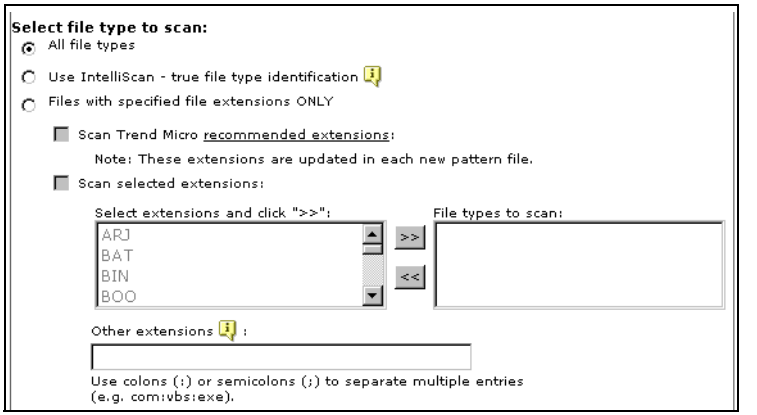
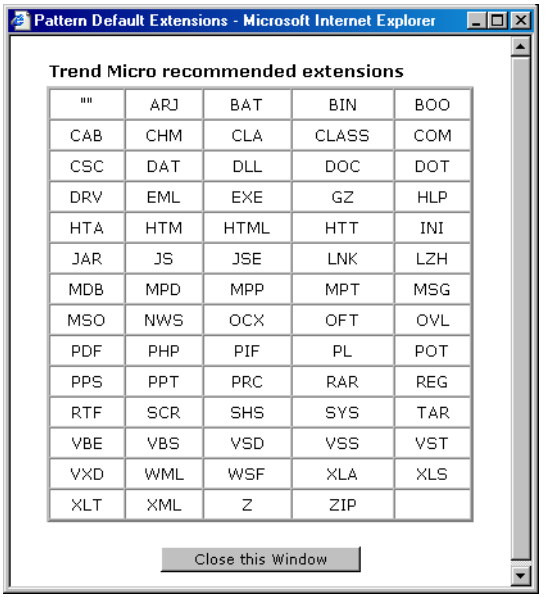


FIGURE 4-3. Selecting file types to scan

The options are:

- **All file types**—Scans all files, except for those specified in the Exclusion List. For additional information on the exclusion List, refer to *What is the Exclusion List?* in the online help.
- **Use IntelliScan**—Scans file headers, then scans the file body only if IntelliScan determines that the file is a type known to harbor malicious code. Hover your cursor over the tooltip icon ( ) for more explanation of this feature.
- **Files with specified file extensions ONLY**—Restricts scanning to selected file extensions. This option also has three sub-options, which you can enable either individually or in combination. These are:

- **Scan Trend Micro recommended extensions** - This option takes advantage of the constantly updated extensions list embedded within the virus pattern. Click the recommended extensions link to view the table of file extensions recommended for scanning. For example:



""	ARJ	BAT	BIN	BOO
CAB	CHM	CLA	CLASS	COM
CSC	DAT	DLL	DOC	DOT
DRV	EML	EXE	GZ	HLP
HTA	HTM	HTML	HTT	INI
JAR	JS	JSE	LNK	LZH
MDB	MPD	MPP	MPT	MSG
MSO	NWS	OCX	OFT	OVL
PDF	PHP	PIF	PL	POT
PPS	PPT	PRC	RAR	REG
RTF	SCR	SHS	SYS	TAR
VBE	VBS	VSD	VSS	VST
VXD	WML	WSF	XLA	XLS
XLT	XML	Z	ZIP	

FIGURE 4-4. Trend Micro recommended extensions for file scanning

- **Scan selected extensions** - You can specify extensions from a list of extensions. To do so:
  - **i.** Select the extension from the **Select extensions...** list.
  - **ii.** Click >> to add the extension to the **File Types to scan** list.
  - **iii.** Click **Save**.

- **Other extensions** - Type custom file extensions in the **Other extensions** text box. Use semicolons (;) or colons (:) to separate entries. For example:

  `LGL;FIN;ADM or LGL:FIN:ADM`

3. Click **Save**.

To remove extensions:

1. Select the extension to be excluded from scanning in the **File types to scan** list.
2. Click << to remove the extension.
3. Click **Save** to apply your settings.

Scanning Compressed Files

Because compressed file scanning is a resource-intensive process, it is important to configure ServerProtect so it can seamlessly scan compressed files and archives while other processes are running.

To scan compressed files:

1. On the left menu, select **Scan Options**, then choose the scan method.
2. Under the **Compressed file** section, select the **Scan compressed files** check box.

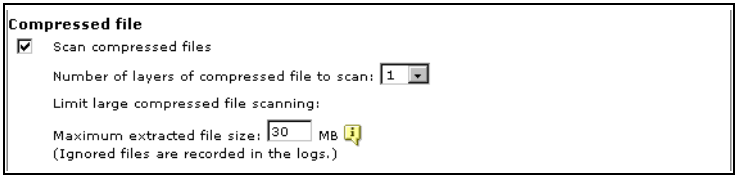


FIGURE 4-5. Compressed file scanning

3. Specify the number of compression layers to scan. The permitted values are from 1 to 20 layers. The default settings are 5 layers for manual and scheduled scanning, and 1 layer for real-time scanning. ServerProtect bypasses files in compression layers that are higher than the number specified.
4. Specify the maximum extracted file size for scanning.

The minimum value you can set is 1MB, while the maximum value is 2,000MB. The default values are 60MB for manual and scheduled scanning, and 30MB for real-time scanning. ServerProtect does not scan files larger than the specified size, but it records an entry about them in the scan log.

5. Click **Save** to apply your settings.

Configuring Real-Time Scanning

When enabled, real-time scanning runs in the background, constantly checking all accessed files. Real-Time Scan differs from manual and scheduled scanning in that it lacks the following options:

- File Types To Scan
- Compressed Files
- Action When Security Risk Found

The features below are configurable.

Enabling Real-Time Scanning

Trend Micro recommends that you keep the Real-time Scanning option enabled at all times.

To enable real-time scanning:

1. Click **Scan Options** > **Real-time Scan** on the left menu.
2. Select the **Enable real-time scan** check box in the **Real-time Scan** screen.
3. Click **Save** to apply the setting.

Note: Trend Micro strongly recommends that you keep real-time scanning enabled; it is enabled by default.

Real-Time Scan Options

Real-time Scan has the following scanning options:

- **Select scan directions**—Choose whether to scan incoming files, outgoing files, and/or running files.
- **Directories to scan—**Choose to scan only specific directories; see *To specify locations to scan:* on page 4-4. Note that you can exclude certain directories from scanning on the Scan Options > Exclusion List screen, for example, you should exclude the ServerProtect quarantine directory from scanning. For additional information on the Exclusion List, refer to *What is the Exclusion List?* in the online help.
- **File types to scan**—Choose file types to be scanned; see *To specify files to scan:* on page 4-6.
- **Compressed file**—Specify handling for compressed files; see *To scan compressed files:* on page 4-8.
- **Action When Security Risk Found**—Click the appropriate action that ServerProtect should take (clean, quarantine, rename, delete, or pass) when it detects a virus or other malware; see *Understanding Virus Actions* on page 4-4 for details of each action. You can select one of three options:
  - **Use ActiveAction**—This is a set of preconfigured scan actions for viruses and other malware. The recommended action for viruses is Clean. The recommended action for Trojans and joke programs is Quarantine. If you are not sure which scan action is suitable for a certain type of security risk, Trend Micro recommends selecting ActiveAction.
  - **Use customized scan action**—Using the table (shown below), create a customized first action for each type of security risk (joke, Trojan, virus, test virus, spyware/grayware, and other). For virus and other threats, select a

second action. For example, for a virus, you might want to select Clean as a first action, and Quarantine as a second action.

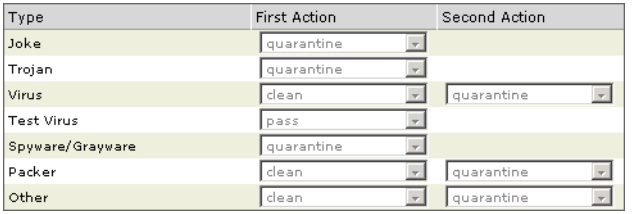


FIGURE 4-6. Specify customized scan actions

- **Use the same action for all types**—These fields allow you to select an action for all files, regardless of file type. The second action applies only to viruses and other security risks, and only when "clean" is selected as the first action.

Note: On rare occasions, malware may damage a file in a way that does not allow cleaning, and as a result, the affected file is not recoverable. To create a backup copy before ServerProtect attempts to clean it, select the **Back up file containing security risk before action is taken** check box.

Setting Scan Target

Real-time scanning can detect viruses within incoming, outgoing, and running files.

Incoming files are those that are being placed on your server, whereas outgoing files are copied or moved from your server to another location. Running files are files that are being executed, such as a program.

View the Real-Time Scan icons on the title bar to verify the status of the scan direction.

FIGURE 4-7. Title bar showing Real-Time Scan with incoming, outgoing, and running file scanning enabled

The icons are shown below:

Scan Target	On	Off
Incoming		
Outgoing		
Running		

TABLE 4-3. Icon display for real-time scanning, by file type

To specify the scanning direction for Real-time Scan:

1. Select the **Incoming files**, **Outgoing files**, and/or **Running files** check boxes, to activate the desired scan target.
2. Click **Save** to apply your settings.

Invoking Manual Scan (Scan Now)

Manual scanning, or Scan Now, is performed on-demand, making it a quick way to verify an infection. There are three ways to perform a manual scan: using saved settings, after configuring scan settings, or through the command line.

To use the saved settings, do one of the following:

- Click 

on the left menu.
- From the task bar on the XWindow main window, click **Start Applications Menu** > **System (Tools)** > **TrendMicro SPLX Administration** > **Manual Scan** > **Start Scan Now**.

To scan after configuring scan settings:

1. Select **Scan Options** > **Manual Scan** on the left menu. The Manual Scan screen displays.
2. Configure the scan settings as required; see *Manual Scan Options* on page 4-14.
3. Click **Save & Scan**. The following confirmation window displays.

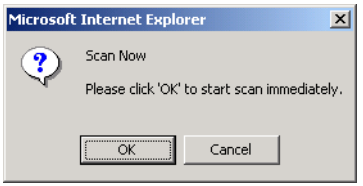


FIGURE 4-8. Scan Now confirmation window

4. Click **OK** to begin the scan.

To invoke manual scan through the command line:

Run the following command:

```
splxmain -m <directory>
```

...where `<directory>` is the directory to scan. Use colons to separate multiple entries. For example, to scan `/temp1` and `/temp2`:

```
splxmain -m /temp1:/temp2
```

After ServerProtect completes the scan, the scan progress window appears showing the status of the scan.

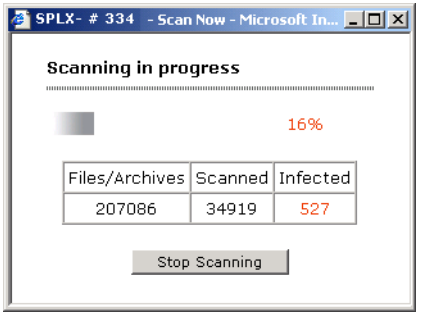


FIGURE 4-9. Scan progress window

Note: A manual scan typically takes a few minutes. You can proceed to other tasks while the scan is in progress.

To stop a manual scan:

- Click **Stop Scanning** on the scan progress window.
- Run the following command:

  ```
  splxmain -n
  ```

- From the task bar on the XWindow main window, click **Start Applications Menu** > **System (Tools)** > **TrendMicro SPLX Administration** > **Manual Scan** > **Stop Scan Now**.

Manual Scan Options

Manual scan has four options to configure. These can be accessed by clicking **Scan Options** > **Manual Scan** on the left menu.

- **Directories to Scan**—Restrict scanning to only specific directories. See *To specify locations to scan:* starting on page 4-4. To save CPU resources, you can exclude mounted drives in your network file system from scanning by clicking the **Use map drive exclusion** check box.
- **File Types to Scan**—Limit scanning to specific file types. See *To specify files to scan:* starting on page 4-6.
- **Compressed File**—Perform a manual scan on compressed files and archives; see *To scan compressed files:* on page 4-8.
- **Action When Security Risk Found**—Click the appropriate action that ServerProtect should take (clean, quarantine, rename, delete, or pass) when it detects a virus or other malware. See *Understanding Virus Actions* on page 4-4 for details of each action. You can select one of three options:
  - **Use ActiveAction**—This is a set of preconfigured scan actions for viruses and other malware. The recommended action for viruses is Clean. The recommended action for Trojans and joke programs is Quarantine. If you are not sure which scan action is suitable for a certain type of security risk, Trend Micro recommends selecting ActiveAction.
  - **Use customized scan action**—Using the table (see Figure 4-6. *Specify customized scan actions* on page 4-11), create a customized first action for each type of security risk (joke, Trojan, virus, test virus, spyware/grayware, and other). For virus and other threats, select a second action. For example, for a virus, you might want to select Clean as a first action, and Quarantine as a second action.

- **Use the same action for all types**—These fields allow you to select a single first and second action for all files, regardless of file type. The second action applies only to viruses and other security risks, and only when the selection for first action is "clean."

Note: On rare occasions, malware may damage a file in a way that does not allow cleaning, and as a result, the affected file is not recoverable. To create a backup copy before ServerProtect attempts to clean it, select the **Back up file containing security risk before action is taken** check box.

Configuring a Scheduled Scan

Scheduled scanning is similar to manual scanning, except it follows a schedule you specify. Scheduled scanning performs a thorough scan of your Linux machine at regular, user-specified intervals. Schedule scans after office hours to avoid interfering with normal operations.

Enabling Scheduled Scan

Trend Micro recommends enabling scheduled scanning to keep servers free of viruses and other security risks.

To enable scheduled scan:

1. Click **Scan Options** > **Scheduled Scan** on the left menu.
2. Select the **Enable scheduled scan** check box.
3. Click **Save** to apply the setting.

Invoking Scheduled Scan

Use `splxmain` to run a scheduled scan immediately. ServerProtect applies the scheduled scan settings saved in `tmsplx.xml`.

To invoke scheduled scan:

Issue the following splxmain command from the command line:

```
splxmain -s
```

Stopping a Scheduled Scan

You can stop a running scheduled scan without disabling it on the Web console. Scanning will resume on the next scheduled date.

Note: Stopping a running scheduled scan will not disable successive scheduled scans. You must log on as *root* to stop a scheduled scan.

To stop a scheduled scan (while it is processing), do one of the following:

- Run the following command:

  ```
  splxmain -t
  ```

- From the task bar on the XWindow main window, click **Start Applications Menu** > **System (Tools)** > **TrendMicro SPLX Administration** > **Scheduled Scan** > **Stop Scheduled Scan**.

Scheduled Scan Options

Scheduled scan has the following scanning options:

- **Directories to Scan**—Restrict scanning to only specific directories; see *To specify locations to scan:* on page 4-4. To save CPU resources, you can exclude mounted drives in your network file system from scanning by clicking the **Use map drive exclusion** check box.
- **File Types to Scan—**Limit scanning to specific file types; see *To specify files to scan:* on page 4-6.
- **Compressed File—**ServerProtect can perform a scheduled scan on compressed files and archives; see *To scan compressed files:* on page 4-8.
- **Action When Security Risk Found**—Click the appropriate action that ServerProtect should take (clean, quarantine, rename, delete, or pass) when it detects a virus or other malware; see *Understanding Virus Actions* on page 4-4 for details of each action. You can select one of three options:
  - **Use ActiveAction**—This is a set of preconfigured scan actions for viruses and other malware. The recommended action for viruses is Clean. The recommended action for Trojans and joke programs is Quarantine. If you are not sure which scan action is suitable for a certain type of security risk, Trend Micro recommends selecting ActiveAction.

- **Use customized scan action**—Using the table (see Figure 4-6.), create a customized first action for each type of security risk (joke, Trojan, virus, test virus, spyware/grayware, and other). For virus and other threats, select a second action. For example, for a virus, you might want to select Clean as a first action, and Quarantine as a second action.
- **Use the same action for all types**—These fields allow you to select a single First and second action for all files, regardless of file type. The second action applies only to viruses and other security risks, and only when "clean" is selected as the first action.

Note: On rare occasions, malware may damage a file in a way that does not allow cleaning, and as a result, the affected file is not recoverable. To create a backup copy before ServerProtect attempts to clean it, select the **Back up file containing security risk before action is taken** check box.

Scan Frequency for Scheduled Scans

You can schedule how often ServerProtect scans your computer on the Scan Options > Scheduled Scan screen.

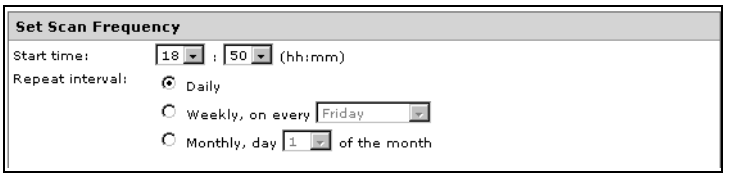


FIGURE 4-10. Set Scan Frequency fields on Scheduled Scan screen

To specify the scan frequency:

Provide the following information:

- **Start time**—Specify the specific hour that the scan starts.
- **Repeat interval**—Specify how often ServerProtect should perform the scan.

Exclusion List

ServerProtect provides the ability to exclude files, directories, and file types from scanning. This feature can be used to avoid scanning quarantine directories and certain virus-proof files. In the unlikely event that the scan engine causes false alarms, you can temporarily include the misidentified file in this list.

There are currently two kinds of exclusion lists, which can be found on the same page:

Directories and Files List - Use this list to exclude whole directories and/or specified files from scanning.

File Types List - This list prevents ServerProtect from scanning specific file types.

In all types of scans except real-time scans, exclusion lists support use of wildcard characters, either the asterisk (*) or question mark (?). An asterisk (*) wildcard matches any number of characters, a question mark (?) wildcard matches only one character.

Note: Each type of scan has its own exclusion list, allowing you better control over how each scan performs.

Viewing Scan Results (Logs)

There are two ways to view scan results:

- Using the Scan Now complete screen (for manual scanning results only)
- Using the Scan and Virus logs

Using the Scan Now Complete Window

The Scan Now complete window provides basic information about the number of files scanned, and the number of infected files detected.

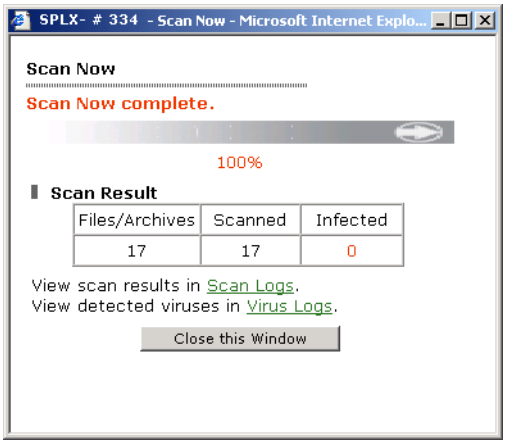


FIGURE 4-11. Scan Now complete window

For detailed information, click the Scan Logs link for details about the scan. Click the Virus Logs link for information about infected files or detected viruses.

Viewing Scan, Virus, and System Logs

ServerProtect offers three types of logs:

Scan Log—The scan log reports type of scans attempted or performed on your servers, including start/end date and time, number of files scanned, and number of detections.

Virus Log—The virus log reports malware detections, including detection date and time, threat name, scan type, action taken and result, and the location of the the source file in which the malware was found.

System Log—The system log reports system events, such as updates of the pattern file and the scan engine and the enabling and disabling of services. The log includes the date and time of the event and the reason for the event.

Note: For more information about logs, and log maintenance, refer to the *What are Logs?* and *Why Maintain Logs?* topics in the online help.

Specifying the Log Directory Location

Scan, virus, and system logs are stored in the log directory. The default location of the log directory is:

```
/var/log/TrendMicro/SProtectLinux
```

To specify a new log directory:

1. Select **Logs** > **Log Directory**.
2. Type the full path of the new location in the **Directory to store logs** field.
3. Click **Save**.

Note: If you change the location of this directory, existing files still remain in the original location.

To view logs:

1. Select **Logs** from the left menu, and select the kind of log you want to view.
2. The Stored Logs section of the screen displays the number of logs currently in the log database, and the date range of the stored logs, if any.
3. Specify the viewing query criteria for the desired logs. The parameters are:
   - **Logs for—**Select among the commonly specified date ranges: **All dates**, **Today**, **Yesterday**, **Past 7 days** or **Past 30 days**. If the period you require is not covered by the above options, choose **Specified date range**; this enables the **Start date** and **End date** fields.
   - **Start date—**Type the earliest log you want to view. Select the **Specified date range** option in **Logs for** to use this criterion. The month-day-year format is used. Alternatively, click the calendar icon () and select a date from the calendar.
   - **End date—**Type the latest log you want to view. Select the **Specified date range** option in **Logs for** to use this criteria. The month-day-year format is used. Alternatively, click the calendar icon () and select a date from the calendar.
   - **Sort logs by—**Specify the order and grouping of the logs. Options for groups are: **Start Date/Time**, **End Date/Time**, **Scan Type**, **Files Scanned**, and **Infected Files**; the order may either be ascending or descending.

- **Logs per page—**From the drop-down menu, select the number of logs to display at a time. Choose a setting that is appropriate for your monitor resolution. The values range from 15 to 200, the default value is 25.

Note: You can increase the number of "logs per page" in the configuration file. See *MaxRetrieveCount* starting on page A-26 for more information.

4. Click **View Log** to begin the query.

See *Scan log* on page 4-21 for an example of the scan log:

From: 07/21/2005 00:25:59

To: 07/26/2005 20:36:49

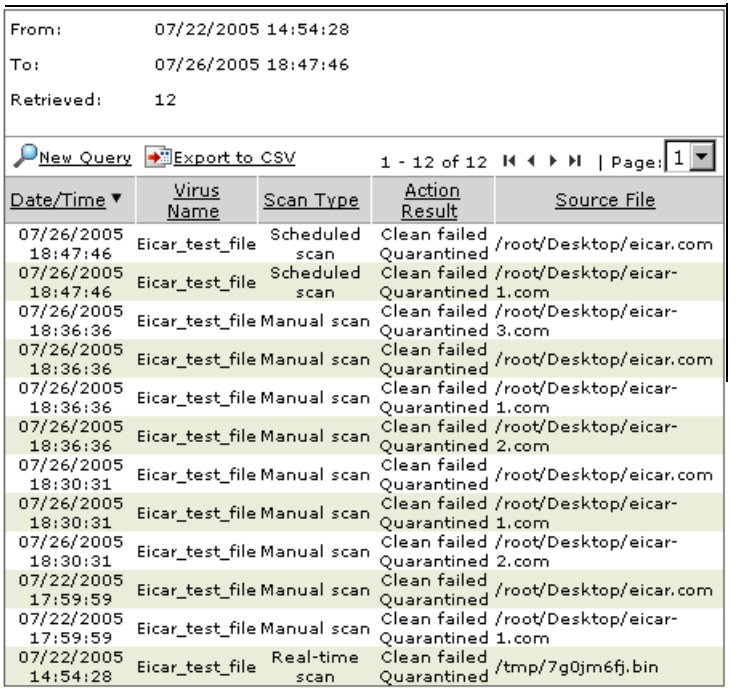
Retrieved: 14

New Query | Export to CSV | 1 - 14 of 14 | Page: 1

Start Date/Time	End Date/Time	Scan Type	Files Scanned	Infected Files
07/26/2005 20:10:21	07/26/2005 20:36:48	Manual scan	133475	0
07/26/2005 18:50:01	07/26/2005 18:50:02	Scheduled scan	2	0
07/26/2005 18:47:45	07/26/2005 18:47:46	Scheduled scan	4	2
07/26/2005 18:40:02	07/26/2005 18:40:02	Scheduled scan	2	0
07/26/2005 18:36:36	07/26/2005 18:36:36	Manual scan	6	4
07/26/2005 18:34:11	07/26/2005 18:34:11	Manual scan	2	0
07/26/2005 18:32:17	07/26/2005 18:32:18	Manual scan	2	0
07/26/2005 18:30:30	07/26/2005 18:30:31	Manual scan	5	3
07/22/2005 17:26:10	07/22/2005 18:01:24	Manual scan	132764	2
07/22/2005 17:23:02	07/22/2005 17:23:03	Manual scan	8	0
07/22/2005 17:22:35	07/22/2005 17:22:36	Manual scan	8	0
07/22/2005 17:21:42	07/22/2005 17:21:43	Manual scan	8	0
07/22/2005 17:19:23	07/22/2005 17:19:23	Manual scan	8	0
07/21/2005 00:00:02	07/21/2005 00:25:58	Scheduled scan	132693	0

FIGURE 4-12. Scan log

See *Virus log* on page 4-22 for an example of the virus log:



From: 07/22/2005 14:54:28

To: 07/26/2005 18:47:46

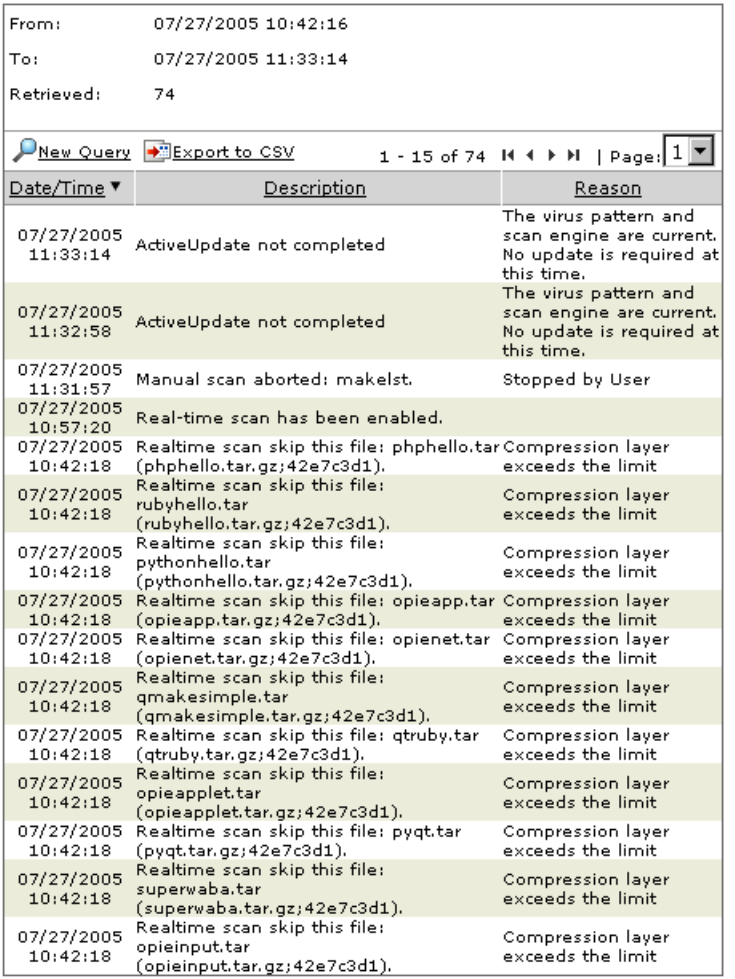
Retrieved: 12

New Query | Export to CSV | 1 - 12 of 12 | Page: 1

Date/Time	Virus Name	Scan Type	Action Result	Source File
07/26/2005 18:47:46	Eicar_test_file	Scheduled scan	Clean failed Quarantined	/root/Desktop/eicar.com
07/26/2005 18:47:46	Eicar_test_file	Scheduled scan	Clean failed Quarantined	/root/Desktop/eicar-1.com
07/26/2005 18:36:36	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar-3.com
07/26/2005 18:36:36	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar.com
07/26/2005 18:36:36	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar-1.com
07/26/2005 18:36:36	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar-2.com
07/26/2005 18:30:31	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar.com
07/26/2005 18:30:31	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar-1.com
07/26/2005 18:30:31	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar-2.com
07/22/2005 17:59:59	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar.com
07/22/2005 17:59:59	Eicar_test_file	Manual scan	Clean failed Quarantined	/root/Desktop/eicar-1.com
07/22/2005 14:54:28	Eicar_test_file	Real-time scan	Clean failed Quarantined	/tmp/7g0jm6fj.bin

FIGURE 4-13. Virus log

See figure Figure 4-14. *System log* on page 4-23, for an example of the system log.



From: 07/27/2005 10:42:16

To: 07/27/2005 11:33:14

Retrieved: 74

New Query | Export to CSV | 1 - 15 of 74 | Page: 1

Date/Time	Description	Reason
07/27/2005 11:33:14	ActiveUpdate not completed	The virus pattern and scan engine are current. No update is required at this time.
07/27/2005 11:32:58	ActiveUpdate not completed	The virus pattern and scan engine are current. No update is required at this time.
07/27/2005 11:31:57	Manual scan aborted: makelst.	Stopped by User
07/27/2005 10:57:20	Real-time scan has been enabled.	
07/27/2005 10:42:18	Realtime scan skip this file: phphello.tar (phphello.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: rubyhello.tar (rubyhello.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: pythonhello.tar (pythonhello.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: opieapp.tar (opieapp.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: opienet.tar (opienet.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: qmakesimple.tar (qmakesimple.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: qtruby.tar (qtruby.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: opieapplet.tar (opieapplet.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: pyqt.tar (pyqt.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: superwaba.tar (superwaba.tar.gz;42e7c3d1).	Compression layer exceeds the limit
07/27/2005 10:42:18	Realtime scan skip this file: opieinput.tar (opieinput.tar.gz;42e7c3d1).	Compression layer exceeds the limit

FIGURE 4-14. System log

To exit the log and start a new log query, click New Query . To export the results of your log query to a .csv file, click Export to CSV . Navigate to the first, previous,

next, and last page of the log query results by clicking the navigation arrows ( ). To refresh the data, click Refresh at the top of the page (not shown in the figures). Upon refresh, the log query screen may add new data to the query, depending on the type of query you selected. For example, if you originally requested today's logs several hours ago, then return to this screen and refresh the screen, any activity that occurred between the previous query and the refresh are added to the log results.

Specifying the Quarantine Directory Location

Occasionally, the scan engine is unable to clean certain files. Also, some files are uncleanable, such as password-protected files. If you do not want to delete uncleanable files, the only recommended alternative is to move the file to the ServerProtect Quarantine Directory. The default location is:

```
/opt/TrendMicro/SProtectLinux/SPLX.Quarantine
```

WARNING! *Files in the Quarantine directory are probably infected. Be careful when accessing files in this directory.*

To specify a Quarantine Directory:

1. Select **Scan Options** > **Quarantine Directory** on the left menu. The Quarantine Directory page displays.
2. Specify the full path of the new location in the **Quarantine directory** field.
3. Click **Save**.

Note: If you change the location of the Quarantine directory, existing files remain in the original location.

Specifying the Backup Directory Location

ServerProtect can back up infected files before Real-time Scan, Scan Now, or Scheduled Scan performs the Clean action (first, select the clean action for the desired scan type(s)). You can change the default backup directory on the Backup Directory screen. The default location is:

```
/opt/TrendMicro/SProtectLinux/SPLX.Backup
```

WARNING! *ServerProtect will not scan files in the backup directory unless you remove it from the Exclusion List of each scan type.*

To specify a Backup Directory:

1. Select **Scan Options** > **Backup Directory**.
2. Type the full path of the new location in the **Backup directory** field.
3. Click **Save**.

Note: If you change the location of this directory, existing files remain in the original location. After specifying a backup directory, ServerProtect adds it to the Exclusion List.

Configuring Notifications

ServerProtect can inform you of specific events that occur on your network, even while you are away from it. It can alert you to virus outbreaks, infections, and system configuration changes, using a variety of notification methods.

This section shows you how to specify the alert events that trigger notifications and the notification methods.

Setting Alert Events

Specify the alert events and the messages ServerProtect will send for each event. This section provides instructions on how to:

- Enable alerts, review default alert notifications
- Modify default notifications to create custom messages

To review/update alert settings:

1. Select **Notification** > **Alert Settings** from the left menu. The Alert Settings screen displays.
2. Select the check boxes of the desired alerts:
   - **Security risk outbreak notification**—This alert triggers a notification if the number of detected viruses and other malware reaches a specified number within a defined unit of time. These outbreak parameters can be set in the appropriate boxes on this screen.
   - **Standard security risk infection notification**—This alert triggers a notification each time ServerProtect detects a security risk on your system.
   - **Notification when real-time scan configuration was modified**—This alert triggers a notification whenever a user modifies the Real-time Scan settings.
   - **Notification when ServerProtect was started**—This alert triggers a notification whenever a user starts ServerProtect service.
   - **Notification when ServerProtect was stopped**—This alert triggers a notification whenever a user stops ServerProtect service.
   - **Notification when virus pattern file is outdated—**This alert triggers a notification if the virus pattern file is a specific number of days old. You can define the age parameter on this page.

3. Each alert event provides a default notification message. See Figure 4-15. *Default messages* on page 4-27 for an example.

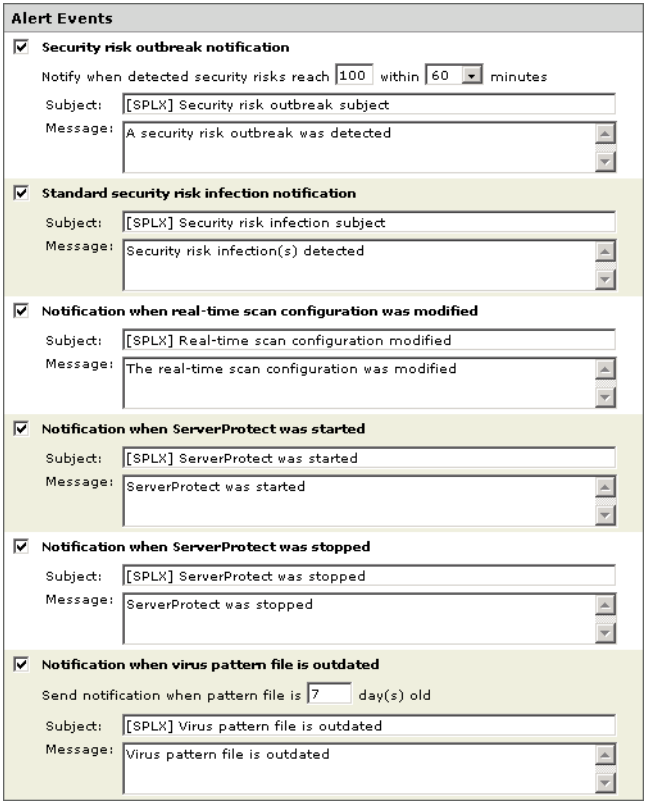


FIGURE 4-15. Default messages

To create custom notification messages:

1. Modify the default notifications by deleting the existing text and typing your new text in the **Message** fields. Your new message cannot exceed 1024 characters.
2. Click **Save** when you are finished. Notifications are sent to the recipient(s) identified on the **Notification** > **Recipients** screen.

Specifying Notification Recipients

ServerProtect allows you to designate multiple recipients for your notifications and use different methods of delivery. This section describes how to:

- Enable SMTP Mail notification
- Modify recipient settings
- Enable SNMP notification

To enable SMTP mail notification:

1. Select **Notification** > **Recipients** from the left menu. The Recipients screen displays.
2. Select the **SMTP Mail Notification** check box.
3. In the **SMTP server** field, type the SMTP server name or its IP address, for example:

   `smtp.server.com` or `192.168.0.0`

4. Specify the mail server listening port in the **Port** field.
5. Type your email address in the **From** field.

Note: Some SMTP servers will not deliver mail if a sender's address is not available.

---

6. Specify the recipient's addresses.

To add a recipient address:

1. Type the recipient's full email address in the address box, for example:

   `yourname@yourCompany.com`

2. Click  to add the entry to the recipients list.

To remove a recipient address:

1. Select an address from the recipients list. To select consecutive addresses, click the first item, press and hold down Shift, and then click the last address. For non-consecutive addresses, press and hold down Ctrl, and then click each item.
2. Click  to remove the selected entry from the recipients list.

3. Specify a character set in the **Character set** field; the default is the Western European character set: iso-8859-1. There are two ways to do this:
   - Type the character set code in the **Character Set** field. For information on other common character sets, see *SMTP Mail Notification Character Sets* on page A-38.
   - Click **Options** to display the Preferred charset screen. Choose the appropriate character set from the Preferred charset screen.
4. Click **Save** to apply the changes.

To modify recipient settings:

1. Select **Notification** > **Recipients** on the left menu
2. Make the appropriate modifications, then click **Save**.

To enable SNMP notification:

1. Select the **SNMP Notification** check box.
2. Type the community name for the message in the **Community name** field.
3. Type the IP address of the SNMP trap server in the **IP address** field.
4. Click **Save**.

Chapter 5

Troubleshooting and Contacting Technical Support

Here you will find answers to frequently asked questions and you will learn how to obtain additional ServerProtect information.

This chapter discusses the following topics

Troubleshooting

The following section provides tips for dealing with issues you may encounter when using ServerProtect for Linux.

Default Password

ServerProtect for Linux does not have a default password. Trend Micro strongly advises you to set one immediately after installation.

Web Console Rejects All Passwords

The Web console may reject any password you try; this may happen as a result of a number of factors:

- **Incorrect password—**Passwords are case-sensitive. For example, “TREND” is different from “Trend” or “trend.”
- **ServerProtect’s customized Apache server does not respond—**Check `splxhttpd` status. For additional information, see *Using splxhttpd Script* on page A-36.
- **Your trial period has expired—**If you do not register ServerProtect within 60 days, the Web console will lock out. If this happens, obtain a serial number for your product, then type it in the **serial number** field on the Logon screen.
- **Java plug-in not installed properly—**This may happen if you are using the Mozilla or Mozilla Firefox browsers. Contact technical support if you need assistance.

ServerProtect 2.5 provides the following debug options:

- **Kernel debugging:** debugs kernel-related actions
- **User debugging:** debugs user-related actions
- **ControlManager debugging:** debugs Trend Micro Control Manager-related actions

Debug Levels

Edit `tmsplx.xml` to define the debug level for each of the debug parameters:

VALUE	KERNEL DEBUGGING (KERNELDEBUGLEVEL)	USER DEBUGGING (USERDEBUGLEVEL*)	TMCM DEBUGGING (CONTROLMANAGERDEBUG†)
0	**Debugging disabled (default)**	Debugging disabled	Debugging disabled
1	Error debugging	**Error debugging: logs, error messages (default)**	**Error debugging (default)**
2	Common debugging	Information debugging– logs error and warning messages	Common debugging
3	Detailed debugging	Common– logs error, warning, and notification-type messages	Detailed debugging
4	n/a	Critical debugging– logs error, warning, notification, and information-type messages	n/a
5	n/a	Detailed debugging– logs error, warning, notification, information, and debug messages	n/a

TABLE 5-1. Debug levels editable with tmsplx.xml

*. `UserDebugLevel` does not control output from startup scripts. They will always be logged regardless of UserDebugLevel value.

†. If `ControlManagerDebug` is enabled, its logs are stored in `/opt/TrendMicro/SProtectLinux/EntityMain.log`.

Note: Detailed debugging produces a large debug file. Trend Micro recommends enabling detailed debugging when replicating an issue, and immediately disabling it after issue replication. Is is also recommended that your logs be on a non-root partition.

Enabling Debug Logs

Modify `tmsplx.xml` and `syslog.conf` to enable ServerProtect debugging.

To enable debug logs:

1. Using a text editor such as `vi`, edit the following configuration files:

   Note: Making incorrect changes to a configuration file can cause serious system errors. Back up `tmsplx.xml` and `syslog.conf` to restore your original settings.

   a. Edit `tmsplx.xml` to define the debug level for each debug parameter (`UserDebugLevel` and `KernelDebugLevel`).

   b. Edit `/etc/syslog.conf` to assign the path and filename where ServerProtect will write debug logs.

      For example:

      - To direct all ServerProtect user debug logs to /path/splx.log, include the following line in `syslog.conf`:

        ```
        local3.* /path/splxUserDebug.log
        ```

      - To direct ServerProtect kernel debug logs to /path/splxKernDebug.log, include the following line in `syslog.conf`:

        ```
        kern.debug /path/splxKernDebug.log
        ```

2. Save and close the configuration file:
3. Query PID.

   For Red Hat, SUSE, and Novell Linux Desktop:

   ```
   ps -ef | grep syslogd
   ```

   For Debian Kernel Debug Mode:

   ```
   ps -ef | grep sysklogd
   ps -ef | grep klogd
   ```

   For Debian User Debug Mode:

   ```
   ps -ef | grep sysklogd
   ```

4. Reload configuration.

   For Red Hat, SUSE, and Novell Linux Desktop:

   ```
   kill -HUP <syslogd PID>
   ```

   For Debian Kernel Debug Mode:

   ```
   kill -HUP <sysklogd PID>
   kill -HUP <klogd PID>
   ```

   For Debian User Debug Mode:

   ```
   kill -HUP <sysklogd PID>
   ```

5. Restart ServerProtect service:

   ```
   /etc/init.d/splx restart
   ```

Note: Detailed debugging produces a large debug file. Trend Micro recommends enabling detailed debugging when replicating an issue, and immediately disabling it after issue replication.

If detailed debugging has to run for a number of days or weeks, use `logrotate` to rotate and compress log files automatically. Refer to the ServerProtect Web console online help *Using logrotate* topic for details on how to compress ServerProtect log files automatically.

Disable Debugging

Modify `tmsplx.xml` and `syslog.conf` to disable ServerProtect debugging.

To disable debugging:

1. Using a text editor such as vi, edit the following configuration files:

   Note: Making incorrect changes to a configuration file can cause serious system errors. Back up `tmsplx.xml` and `syslog.conf` to restore your original settings.

2. Press **ESC**, and then type save and close tmsplx.xml:
3. Delete or comment out the debug path and filename in `/etc/syslog.conf`.
4. Restart ServerProtect service:

   ```
   /etc/init.d/splx restart
   ```

5. Query PID.

   For Red Hat, SUSE, and Novell Linux Desktop:

   ```
   ps -ef | grep syslogd
   ```

   For Debian:

   ```
   ps -ef | grep sysklogd
   ps -ef | grep klogd
   ```

6. Reload configuration.

   For Red Hat, SUSE, and Novell Linux Desktop:

   ```
   kill -HUP <syslogd PID>
   ```

   For Debian:

   ```
   kill -HUP <sysklogd PID>
   kill -HUP <klogd PID>
   ```

Before Contacting Technical Support

Before contacting technical support, here are two things you can quickly do to try and find a solution to your problem:

- **Check your documentation**—The manual and online help provide comprehensive information about ServerProtect. Search both documents to see if they contain your solution.
- **Visit our Technical Support Web site**—Our Technical Support Web site, called Knowledge Base, contains the latest information about all Trend Micro products. The support Web site has answers to previous user inquiries.

  To search the Knowledge Base, visit

  `http://esupport.trendmicro.com`

Contacting Technical Support

In addition to telephone support, Trend Micro provides the following resources:

Email support

`support@trendmicro.com`

Help database—configuring the product and parameter-specific tips

Readme—late-breaking product news, installation instructions, known issues, and version specific information

Knowledge Base—technical information procedures provided by the Support team:

`http://esupport.trendmicro.com/`

Product updates and patches

`http://www.trendmicro.com/download/`

To locate the Trend Micro office nearest you, visit the following URL:

`http://www.trendmicro.com/en/about/contact/overview.htm`

To speed up the problem resolution, when you contact our staff please provide as much of the following information as you can:

- Product Activation Code
- ServerProtect Build version
- Exact text of the error message, if any
- Steps to reproduce the problem

Sending Infected Files to Trend Micro

You can send viruses, infected files, Trojan horse programs, and other malware to Trend Micro. More specifically, if you have a file that you think is some kind of malware but the scan engine is not detecting it or cleaning it, you can submit the suspicious file to Trend Micro using the following Web address:

`subwiz.trendmicro.com`

Please include in the message text a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any viruses it may contain and return the cleaned file to you, usually within 48 hours.

TrendLabs™

Trend Micro TrendLabs is a global network of antivirus research centers that provide continuous 24x7 coverage to Trend Micro customers around the world.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

`http://www.trendmicro.com/en/security/trendlabs/overview.htm`

About Software Updates

After a product release, Trend Micro often develops updates to the software, to enhance product performance, add new features, or address a known issue. There are different types of updates, depending on the reason for issuing the update.

The following is a summary of the items Trend Micro may release:

- **Hot fix—**A hot fix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes don't (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).
- **Security Patch—**A security patch is a hot fix focusing on security issues that is suitable for deployment to all customers. Windows security patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Patch—**A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Service Pack—**A service pack is a consolidation of hot fixes, patches, and feature enhancements significant enough to be considered a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

Check the Trend Micro Knowledge Base to search for released hot fixes:

`http://esupport.trendmicro.com`

Consult the Trend Micro Web site regularly to download patches and service packs:

`http://www.trendmicro.com/download`

All releases include a readme file with the information needed to install, deploy, and configure your product. Read the readme file carefully before installing the hot fix, patch, or service pack file(s).

Known Issues

Known issues are features in your ServerProtect software that may temporarily require a workaround. Known issues are typically documented in section 9 of the Readme document you received with your product. Readme's for Trend Micro products can also be found in the Trend Micro Update Center:

`http://www.trendmicro.com/download/`

Known issues can be found in the technical support Knowledge Base:

`http://esupport.trendmicro.com`

Note: Trend Micro recommends that you always check the Readme text for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

Other Useful Resources

Trend Micro offers a host of services via its Web site, http://www.trendmicro.com.

Internet-based tools and services include:

- Virus Map- monitor virus incidents around the world

Virus risk assessment– the Trend Micro online virus protection assessment program for corporate networks

Appendix

This appendix provides additional information about ServerProtect command line configuration tools, and additional product information.

This appendix discusses the following topics:

Accessing ServerProtect Man Pages

ServerProtect man pages contain relevant ServerProtect command and configuration information.

ServerProtect man pages are:

- `tmsplx.xml`: explains the ServerProtect configuration parameters
- `splxmain`: includes the splxmain command information
- `splx`**:** explains the ServerProtect startup script and includes error messages
- CMconfig: explains usage of this utility
- RemoteInstall: explains the usage and parameters of this utility

To access ServerProtect man pages, type the following at the command line:

```
man {manpage}
```

For example:

```
man tmsplx.xml
```

Understanding `tmsplx.xml`

This section includes descriptions of the parameters for configuring ServerProtect.

Note: Making incorrect changes to the configuration file can cause serious system errors. Back up `tmsplx.xml` to restore your original settings.

The configuration file is located in:

```
/opt/TrendMicro/SProtectLinux/tmsplx.xml
```

Entries adhere to the following format:

```
<P Name="key" Value="value"/>
```

Each of the following groups is a collection of keys with similar functionality:

- Scan Group Keys
- ActiveUpdate Group Keys
- SOURCEINFO Group Keys
- DESTINFO Group Key

Note: The `SOURCEINFO` group contains parameters to enable or disable advanced component download options via ActiveUpdate. Refer to *Enable/Disable Advanced ActiveUpdate Options* topic in the online help.

- Notification Group Keys
- Configuration Group Keys
- GUIPassword Group Key
- Logs Group Keys
- Registration Group Keys

The criteria for editing the configuration file are:

- Each parameter must begin with (<) and end with (/>)
- All keys and values must be surrounded by double quotes (" ")
- Use a colon (:) to separate multiple values within the same key

  For example:

  ```
  /var/tmp:/home/samba:/tmp
  ```

After modifying and saving the `tmsplx.xml` file, restart ServerProtect.

To restart ServerProtect:

Type the following at the command line:

```
su root -
/etc/init.d/splx restart
```

Trend Micro recommends backing up the customized `tmsplx.xml` file in case it gets corrupted. The `tmsplx.xml.tmplate` file is a copy of the default configuration file; use this file to revert to the initial settings. Use the `tmsplx.xml.tmplate` file as a backup for the configuration file.

Note: Whenever you replace an existing configuration file with the `tmsplx.xml.tmplate` file, the ServerProtect Web console will require re-applying your Activation Code/serial number, because it is stored in the configuration file.

The configuration file contains subsections that correspond to the different modules in the ServerProtect software.

`Scan` Group Keys

This set of keys controls virus-scanning operations. You can configure Real-time Scan, Scheduled Scan, and Manual Scan individually.

Scheduled scans run at predetermined times using `cron` for Debian, SUSE, and Novell Linux Desktop or `crond` for Red Hat. ServerProtect converts the frequency and time information specified in the `tmsplx.xml` file into valid `/etc/cron.d/splx` entries. You can specify to scan files by directory, or by extension, using either a "scan all files except the specified ones" or a "do not scan any files other than the specified ones" logic.

Note: If there is a conflict, exclusion settings take precedence over inclusion settings.

`RealtimeScan`

This key enables/disables Real-time Scan.

The valid values are:

- `0` disable
- `1` scan incoming files (default value)
- `2` scan outgoing files
- `3` scan both incoming and outgoing files
- `4` scan running files
- `5` scan running and incoming files

6 scan running and outgoing files

7 scan running, incoming, and outgoing files

RealtimeIncludeDirList, ScheduledIncludeDirList, ManualIncludeDirList

Use these keys to include specific directories in a scan. Type the full path of the desired directories, and then separate them with a colon (:). For example, to include the `tmp` and `etc` directories in Real-time Scan type the following:

```
<P Name="RealtimeIncludeDirList" Value="/tmp:/etc"/>
```

Note: Use the null (default) value to scan all directories.

RealtimeIntelliScan, ScheduledIntelliScan, ManualIntelliScan

Use this key to turn IntelliScan on or off from within the configuration file. The default value = 0 (off).

ScheduledMapDriveExclusion, ManualMapDriveExclusion

Use this key to turn Map Drive Exclusion feature on or off within the configuration file. The values are 0 = disable Map Drive Exclusion, 1 = enable Map Drive Exclusion.

RealtimeIncludeExtList, ScheduledIncludeExtList, ManualIncludeExtList

Use these keys to add specific file types (identified by extension) in a scan. Use a colon (:) to separate different file types. You can use small and capital letters interchangeably when typing the file types. For example, to include the `BIN` and `RPM` file types in Real-time Scan type the following:

```
<P Name="RealtimeIncludeExtList" Value="BIN:RPM"/>
```

Note: Use the null (default) value to scan all file types.

RealtimeIncludeTMExtList, ScheduledIncludeTMExtList, ManualIncludeTMExtList

Use these keys to select scanning of all file types, or scanning of file types by extension (for which Trend Micro recommends scanning). The valid values are:

`0` (default value) Scan all file types

`1` Scan files with specified extensions

RealtimeExcludeDirList, ScheduledExcludeDirList, ManualExcludeDirList

Use these keys to exclude certain directories from scanning. Type the full path of the desired directories, and then separate them with a colon (:).

Note: If the value is null, all directories will be part of the scan.

The default values are:

```
/dev:/proc:/var/spool/mail:/var/mail:var/spool/myqueue
:/var/spool/mqueue.iscan
/opt/TrendMicro/SProtectLinux/SPLX.Backup
/opt/TrendMicro/SProtectLinux/SPLX.Quarantine
```

RealtimeExcludeFileList, ScheduledExcludeFileList, ManualExcludeFileList

Use these keys to exclude individual files from scanning. Type the full path of the desired files, and then separate them with a colon (:). For example, to exclude a file called `fm.txt` under the `etc` directory from Real-time Scan type the following:

```
<P Name="RealtimeExcludeFileList" Value="/etc/fm.txt"/>
```

Note: If the value is null (default), all files will be part of the scan.

RealtimeExcludeExtList, ScheduledExcludeExtList, ManualExcludeExtList

Use these keys to exclude file types (identified by extension) from a scan. Use a colon (:) to separate the different file types For example, to exclude the `BIN` and `TXT` file types in a Real-time Scan type the following:

<P Name="RealtimeExcludeExtList" Value="BIN:TXT"/>

Note: You can use small and capital letters interchangeably when typing the file types.

RealtimeCustomizedAction, ScheduledCustomizedAction, ManualCustomizedAction

These keys specify the default values for customized actions for specific types of security risks, as seen in the "Action When Security Risk Found" sections of the Real-time Scan, Scheduled Scan, and Manual Scan screens.

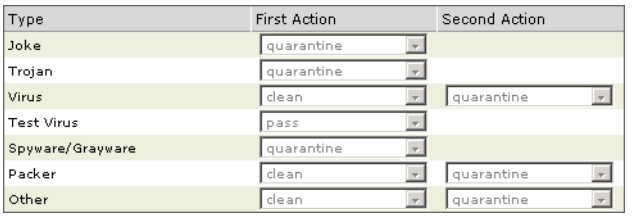


FIGURE A-1. Default values for first/second action when selecting customized scan action

For viruses and other threats, a second action can be specified.

The following values apply:

0 = Pass (take no action)
1 = Rename infected files by appending the extension specified by the `FileExtentionToRename` key.
2 = Quarantine
3 = Clean
4 = Delete

Therefore, the default custom settings are as follows:

Joke = 2-0
Trojan = 2-0
Virus = 3-2
Test Virus = 0-0
Spyware = 2-0
Other = 3-2
Disable customized actions = 0

`RealtimeAllTypesAction, ScheduledAllTypesAction, ManualAllTypesAction`

These keys specify the default values for actions for all types of security risks, as seen in the "Action When Security Risk Found" sections of the Real-time Scan, Scheduled Scan, and Manual Scan screens.

FIGURE A-2. Default values for first/second action when selecting "all types" scan action

For viruses and other threats only, a second action can be specified.

The following values apply:

0 = Pass (take no action)
1 = Rename infected files by appending the extension specified by the `FileExtentionToRename` key.
2 = Quarantine
3 = Clean
4 = Delete

Therefore, the default custom settings are as follows:

All Types = 3-2
Disable all types actions = 0

Note: When the RealtimeCustomizedAction, ScheduledCustomizedAction, and ManualCustomizedAction keys are set to zero and the RealtimeAllTypesAction, ScheduledAllTypesAction, ManualAllTypesAction are also set to zero, then Active Action is selected on the Real-time Scan, Scheduled Scan, and Manual Scan screens.

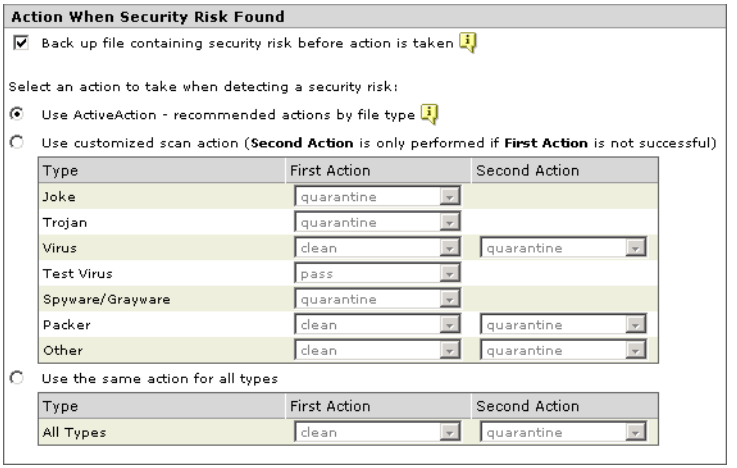


FIGURE A-3. ActiveAction is enabled when settings for Customized and All Types are set to 0

RealTimeScanArchived, ScheduledScanArchived, ManualScanArchived

This key is not used at this time.

RealtimeScanCompressed, ScheduledScanCompressed, ManualScanCompressed

Use these keys to enable/disable compressed file scanning. The valid values are:

`0` disable scan of compressed files

`1` enable scan of compressed files (default value)

RealtimeCompressionLayer, ScheduledCompressionLayer, ManualCompressionLayer

These keys determine the default number of compression layers ServerProtect scans. The valid values are `1` through `20`, the default value for Real-time Scan is `1`, for Scheduled Scan and Manual Scan the default is `5`.

Note: Using low values reduces the performance impact of scanning, however at the expense of less protection.

RealtimeCompressedFileSize, ScheduledCompressedFileSize, ManualCompressedFileSize

These keys determine the maximum original size (without compression or archiving) of compressed or archived files to scan. This value is in megabytes, the maximum value is `2000`, and the default value for Scheduled Scan and Manual Scan is `60`. The default value for Real-time Scan is `30`. For example, if the `RealtimeCompressedFileSize` value is `40`, only compressed files that are 40MB or smaller before compression will be scanned in real time:

```
<P Name="RealtimeCompressedFileSize" Value="40"/>
```

Note: Using small values can improve scan performance, but at the expense of less protection.

RealtimeCleanSave, ScheduledCleanSave, ManualCleanSave

These keys enable/disable backing up files before a clean operation. The valid values are:

`0` disable file backup

`1` enable file backup (default)

ScheduledNice, ManualNice

This key is used to set process scheduling priority. The values are:

-20 = highest
19 = lowest

DirToMove

This key shows the directory to which files will be moved when a virus is found and the **AllTypesAction** or **CustomizedAction** keys are set to `Quarantine`. The default value is:

```
/opt/TrendMicro/SProtectLinux/SPLX.Quarantine
```

DirToSave

This key determines the directory where infected files are stored before a clean operation. The default value is:

```
/opt/TrendMicro/SProtectLinux/SPLX.Backup
```

FileExtensionToRename

The file extension that is appended to an infected file when the **AllTypesAction** or **CustomizedAction** fields are set to `Rename`. The default is `vir`.

ActionForTimeout

This key is not currently in use.

VirusOutbreak

This key enables/disables sending a notification when there is a virus outbreak. The valid values are:

`0` disable sending virus outbreak notifications

`1` enable sending virus outbreak notifications (default value)

Note: ServerProtect will not send any alert notifications until the number of infected files reaches the number specified in the VirusOutbreakCount key.

VirusOutbreakPeriod

This key sets the time interval, in minutes, between virus outbreak notifications. The valid values are: `5`, `10`, `30`, `60`, `120`, and `240`; the default value is `60`. This key has no effect if the `VirusOutbreak` key is disabled.

VirusOutbreakCount

This key controls the number of infected files required for sending a virus outbreak notification. The valid values are `1` through `1000`, and the default value is `100`. This key has no effect if the `VirusOutbreak` key is disabled.

AlertVirusInfection

This key controls whether ServerProtect sends an alert notification when it finds infected files on the system. The valid values are:

- `0` disable sending an alert notification when ServerProtect finds an infected file
- `1` enable sending an alert notification when ServerProtect finds an infected file (default value)

AlertRealtimeConfigChange

This key controls whether ServerProtect sends an alert notification whenever you modify a Real-time Scan configuration setting. The valid values are:

- `0` disable sending an alert notification whenever a Real-time Scan configuration setting changes
- `1` enable sending an alert notification whenever a Real-time Scan configuration setting changes (default value)

AlertServerProtectOn and AlertServerProtectOff

These keys controls whether ServerProtect send an alert notification whenever **splx** service stops or restarts. The valid values are:

- `0` disable sending an alert notification whenever **splx** service stops or restarts
- `1` enable sending an alert notification whenever **splx** service stops or restarts (default value)

AlertPatternOutOfDate

This key controls whether ServerProtect send an alert notification whenever the pattern file is out-of-date.

- `0` disable sending an alert notification whenever the pattern file is out-of-date
- `1` enable sending an alert notification whenever the pattern file is out-of-date (default value)

AlertPatternOutOfDatePeriod

This key sets the frequency, in days, for checking whether the pattern file is up to date. The valid values are `1` though `1000`, and the default value is `7`. For example, to have ServerProtect check whether the pattern file is up to date once every `7` days, type the following:

```
<P Name="AlertPatternOutOfDatePeriod" Value="7"/>
```

Schedule

This key sets how often a scheduled scan runs. The valid values are:

- `0` no scheduled scan jobs (default)
- `2` scheduled scan jobs run once every day
- `3` scheduled scan jobs run once every week
- `4` scheduled scan jobs run once every month

ScheduledTime

This key shows when a scheduled scan runs based on the 24-hour clock. The default value is `00:00:00` (midnight).

For example, to run a scheduled scan at 1:30 p.m. type the following:

```
<P Name="ScheduledTime" Value="13:30:00"/>
```

ScheduledWDay

This key sets the day of week a scheduled scan runs when the value of the `Schedule` key is `3` (once every week). The valid values are `Monday`, `Tuesday`,

`Wednesday`, `Thursday`, `Friday`, `Saturday`, `Sunday`, and the default value is null.

`ActiveUpdate` Group Keys

This set of keys specifies various options related to the Trend Micro Update server. Keys in this group provide information about the current ServerProtect status.

Note: Before making any changes to any key in this group, contact Trend Micro technical support for assistance.

`EngineLastUpdateTime`

This key should not be modified by users.

`EngineType`

This key should not be modified by users.

`EngineVersion`

This key should not be modified by users.

`PatternLastUpdateTime`

This key should not be modified by users.

`PatternType`

This key should not be modified by users.

`PatternVersion`

This key should not be modified by users.

`PatternDate`

This key should not be modified by users.

ProductType

This key should not be modified by users.

ProductVersion

This key should not be modified by users.

Language

This key should not be modified by users.

Platform

This key should not be modified by users.

ScheduledNOption

This key controls the type of components updated when ServerProtect performs a Scheduled Update. The valid values are:

1 update virus pattern

2 update scan engine

3 update virus pattern and scan engine (default value)

ManualNOption

This key controls the type of components updated when ServerProtect performs a manual update. The valid values are:

1 update virus pattern

2 update scan engine

3 update virus pattern and scan engine (default value)

Option

Options for ActiveUpdate. This key is set to AU_OPTION and cannot be changed.

Schedule

This key specifies the schedule for a scheduled update. The valid values are:

`0` no schedule

`1` hourly updates

`2` daily updates (default)

`3` weekly updates

The following three keys control the time and dates for the above schedule.

ScheduledTime

This key specifies the time of day for scheduled updates, using a 24-hour clock. Use this key when the value of the `Schedule` key is `1`, `2`, or `3`.

RandomizedUpdate

This key specifies use of the randomized ActiveUpdate feature to assist with load balancing on the ActiveUpdate server. This feature is enabled by default, with a default interval of 2 hours from the update time specified. A value of `0` disables the randomized update feature. The range of values is `0` through `12`.

UpdateRetryNum

This key specifies the number of times that the ActiveUpdate server will attempt to update the pattern files and scan engine. A value of `0` disables the update retry. The range of values is `0` through `3`. The default value is 3.

UpdateRetryInterval

This key specifies the interval between retry attempts in minutes. The range is `10` through `60`, the default = `10`.

`SOURCEINFO` Group Keys

This set of keys determines the source from which ServerProtect downloads pattern files, program updates, and outbreak prevention policies.

DefaultSource

This key contains the URL from which updates are downloaded. The default value for ServerProtect 2.5 differs based upon whether or not ServerProtect is registered to Trend Micro Control Manager (TMCM).

When ServerProtect is registered to TMCM, the default value is:

```
http://xxx.xxx.xxx.xxx/TVCSDownload/ActiveUpdate
```

...where xxx.xxx.xxx.xxx is the Control Manager IP address.

When ServerProtect is not registered to TMCM, the default value is:

```
http://splx-p.activeupdate.trendmicro.com/activeupdate
```

WARNING! *Do not modify this value unless Trend Micro notifies you that the URL for updates has changed.*

DigSig

This key instructs ServerProtect whether to apply digital signature when downloading components from download source. The valid values are:

`0` disable digital signature download (default)

`1` enable digital signature download

SrvAuth

This key instructs ServerProtect whether to apply HTTP authentication when downloading components from an HTTP source. The valid values are:

`0` disable digital signature download (default)

`1` enable digital signature download

Merge

This key instructs ServerProtect whether to apply pattern file merging when downloading virus pattern file from ActiveUpdate. The valid values are:

`0` disable digital signature download

`1` enable digital signature download (default)

Source

This key contains an alternate source for downloading updates. If the value of this key is not null, ServerProtect uses this source in preference to `DefaultSource`**.** The value of the `Source` key may be either a URL or a local path. The default value for this key is null. For example:

```
http://????.com/download
```

ProxyUsername

If your proxy server requires authentication, this key contains the user name. The default value is null.

ProxyPassword

If your proxy server requires authentication, this key contains the password. The default value is null. You can modify this value using the Web console and splxmain. See *Using splxmain* on page A-30.

Proxy

This key contains the IP address or domain name of your proxy server. The default value is null. For example:

```
proxy.company.com
```

UseProxy

This key indicates a proxy server is required to access the ActiveUpdate URL specified in `Source` or `DefaultSource`. The valid values are:

`0` do not use a proxy server (default)

`1` use a proxy server

If you assign a value of `1` to the `UseProxy` key, set the proxy address using the `Proxy` key, and if required, the username, password, and port number.

ProxyPort

This key contains the proxy port number. The default value is null.

DESTINFO Group Key

This key contains the default directory path for the ServerProtect for Linux software. The default value is:

```
/opt/TrendMicro/SProtectLinux
```

Notification Group Keys

You can configure ServerProtect to send notifications for various security events. This set of keys specifies the contents and recipients of notifications. Use the keys in the Scan group to enable or disable sending of notifications.

Specify the sender and receiver(s) email addresses, and the SMTP or SNMP server. These settings are for all types of security event notifications.

Type

This key indicates the delivery method for notifications. The valid values are:

"" (null) default value

SMTP use an SMTP server

SNMP use the SNMP protocol

SMTP:SNMP use both delivery methods

SmtpServer

This key indicates the domain name or IP address of the SMTP server. For example:

```
mail.company.com
```

If the value of the Type key is either SMTP or SMTP:SNMP, the value of this key must not be null. The default value is null.

SmtpPort

This key contains the port number of the SMTP server. The valid values are 1 through 65535. The default value is 25.

SmtpFrom

This key contains the originating email address for sending notification emails. For example:

```
administrator@company.com
```

The default value is null.

Note: Some SMTP servers will not deliver email, unless there is a valid originating email address.

SmtpTo

This key contains the notification recipients. You can specify multiple accounts by separating them with colons. For example:

```
pd@company.com:fm@company.com
```

Note: The default value of this key is null.

SmtpTimeout

The SMTP timeout value, in seconds. The default is 15.

SmtpCharset

This key specifies the character set ServerProtect uses to encode notification emails. For information on other commonly used character sets. See *SMTP Mail Notification Character Sets* on page A-38 for additional information. The default value is `iso-8859-1` (Latin 1 Western European).

SnmpHostname

This key contains the host name or IP address of the SNMP manager. For example:

```
snmp.company.com
```

If the value of the `Type` key is either `SNMP` or `SMTP:SNMP`, the value of this key must not be null. The default value is null.

SnmpCommunity

This key contains the SNMP community name. The default value is `public`. If the value of the `Type` key is either `SNMP` or `SMTP:SNMP`, the value of this key must not be null.

VirusOutbreakSubject

This key contains the subject line of the virus outbreak notification. The default value is:

```
[SPLX] Security risk outbreak subject
```

VIRUSOUTBREAKMESSAGE

This key contains the message body text of the virus outbreak notification. The default value is:

```
A security risk outbreak was detected
```

VirusInfectionSubject

This key contains the subject line of the virus infection notification. The default value is:

```
[SPLX] Security risk infection subject
```

VIRUSINFECTIONMESSAGE

This key contains the message body text of the virus infection notification. The default value is:

```
Security risk infection(s) detected
```

RealtimeConfigChangeSubject

This key contains the subject line of the Real-time Scan configuration change notification. The default value is:

```
[SPLX] Real-time scan configuration modified
```

REALTIMECONFIGCHANGEMESSAGE

This key contains the message body text of the Real-time Scan configuration change notification. The default value is:

```
The real-time scan configuration was modified
```

ServerProtectOnSubject

This key contains the subject line of the ServerProtect on notification. The default value is:

```
[SPLX] ServerProtect was started
```

ServerProtectOffSubject

This key contains the subject line of the ServerProtect off notification. The default value is:

```
[SPLX] ServerProtect was stopped
```

SERVERPROTECTONMESSAGE

This key contains the message body text of the ServerProtect on notification. The default value is:

```
ServerProtect was started
```

SERVERPROTECTOFFMESSAGE

This key contains the message body text of the ServerProtect off notification. The default value is:

```
ServerProtect was stopped
```

PatternOutOfDateSubject

This key contains the subject line of the pattern out-of-date notification. The default value is:

```
[SPLX] Virus pattern file is outdated
```

PATTERNOUTOFDATEMESSAGE

This key contains the message body text of the pattern out-of-date notification. The default value is:

```
Virus pattern file is outdated
```

MaxItemNumber

The maximum number of notifications to be queued in the notification queue. The default value is 1000.

`Configuration` Group Keys

The keys in this group control configuration settings.

ControlManagerDebug

The range is 0 to 3, with 0 meaning “disable.” The default value is 1. For more information, see Table 5-1, “Debug levels editable with tmsplx.xml,” on page 5-3.

ThreadNumber

This key should not be modified by users.

UserDebugLevel

This key should not be modified by users.

KernelDebugLevel

This key should not be modified by users.

MaxCacheItem

This key should not be modified by users.

MaxListItem

This key should not be modified by users.

MaxDirItem

This key should not be modified by users.

MaxExtItem

This key should not be modified by users.

MaxExcDirItem

This key should not be modified by users.

MaxExcFilItem

This key should not be modified by users.

MaxExcExtItem

This key should not be modified by users.

WaitqTimeout

This key should not be modified by users.

VsapiTimeout

This key should not be modified by users.

MaxExcPid

This key should not be modified by users.

MaxVscPid

This key should not be modified by users.

MaxPathLen

This key should not be modified by users.

MaxCmdLen

This key should not be modified by users.

GUIPassword Group Key

This key contains information about the password for the user interface. This key should not be modified by users.

Logs Group Keys

The keys in this group control where the ServerProtect log files are stored, and how often ServerProtect deletes the log files. You should choose values to ensure you keep a reasonable history for studying security events.

ServerProtect deletes the log directory according to the schedule you specify by running the `splxmain -g` command. You can disable purging completely by setting `Schedule=0`. Some administrators prefer to delete the log files manually so they can save them to CD or other media before deleting them.

Note: Log files can grow quite large, so it is important to delete them regularly.

Whenever ServerProtect runs `splxmain -g` automatically or manually through the command line, ServerProtect deletes logs that are older than the number of days specified in the `MaxLogDay` key.

Schedule

This key specifies the frequency for the scheduled log deletions. The valid values are:

`0` disable automatic deletions of the log file

`1` enable (default value)

ScheduledTime

This key specifies the time of day for log deletions, using a 24-hour clock. The default value is `02:00:00` (2 AM).

LogDirectory

This key stores the full path of the directory where all ServerProtect log files (Scan log, Virus log, and System log) are stored. The default value is:

```
/var/log/TrendMicro/SProtectLinux
```

MaxLogDay

This key specifies the number of days that ServerProtect retains logs before purging them. The valid values are `1` through `1000`. The default value is `60`.

Note: This value is large to protect new users from inadvertently losing history. Trend Micro recommends that you back up your log files weekly and reduce the `MaxLogDay` value.

MaxRetrieveCount

This key allows you to specify the maximum number of log entries to retrieve. In ServerProtect releases prior to 2.5, only 1000 entries could be retrieved via the screens in the Web Console. In response to customer requests, this limit is now configurable by editing the tmsplx.xml file. This key has a value range from 200 to 65535. The default value is 1000, which matches the behavior of earlier releases.

Note: This limit applies only to referencing logs via the Web Console; all entries can be viewed by viewing the files directly, unless the log has been purged.

The Web Console also allows you to choose how many log entries display per page. The range is from 15 to 200, the default is 25.

Registration Group Keys

The keys in this group contain data used by ServerProtect for product registration and activation.

SerialNumber

This key contains the ServerProtect serial number in encrypted format. This key should not be modified by users.

InstallationDate

This key contains the installation date.

Backing Up and Verifying the Configuration File

Whenever you make a change to ServerProtect for Linux configuration, Trend Micro recommends that you make a backup copy of the configuration file. A suggested file naming convention follows:

`tmsplx.xml`—The current configuration file.
`tmsplx.xml.bak`—The most recent backup (the contents should always match `tmsplx.xml`).
`tmeplx.xml.template`—Theconfiguration file template.

To verify that the key values in the tmsplx.xml file are not corrupt:

At the command line, type the following:

```
/opt/TrendMicro/SProtectLinux/SPLX.util/xmlvalidator
```

Using RemoteInstall.conf

Figure 4. *RemoteInstall.conf keys, default values, and descriptions* on page A-28 lists all of the keys in the `RemoteInstall.conf` file, including whether they are configurable and their default values.

Key	Default value	Description
[DeployOption]	1	1 - ServerProtect 2.5 package deployment and installation 2 - ServerProtect configuration file deployment 3 - KHM module deployment
[Package Name]	SProtectLinux-2.5.i686.bin	Indicates the ServerProtect installation file path for package deployment
[SerialNumber]	(empty)	The ServerProtect 2.5 serial number for installation. Used for package deployment.
[ConfigFilePath]*	config/tmsplx.xml	Indicates the configuration file path. Used for configuration file deployment.
[XMLvalidatorPath]	config/xmlvalidator	Indicates the XMLvalidator script path. Used for configuration file deployment.
[XMLdeployerPath]	config/xmldeployer	Indicates the XMLdeployer program file path. Used for configuration file deployment.
[KHMPath]	KHM.module/RHEL4/splx-mod-2.6.9-22.0.2.ELsmp.o	Indicates KHM file path. Used for KHM deployment. Limit is one KHM file per KHM deployment.
[ConnectTimeOut]	30	Specifies the timeout (in seconds) used when connecting to the ssh server, instead of using the default system TCP timeout. Used only when the target is down or unreachable, not when it refuses the connection.
[ConnectRetry]	2	Used to retry frequency of ssh connection.
[AliveInterval]*	30	Sets a timeout interval in seconds after which if no data has been received from the server, ssh will send a message through the encrypted channel to request a response from the server. This option applies to protocol version 2 only. See **ssh_config** man page, key word *ServerAliveInterval*.

TABLE A-4. `RemoteInstall.conf` **keys, default values, and descriptions**

Key	Default value	Description
[AliveCountMax]	2	Sets the number of server alive messages that can be sent without ssh receiving any messages back from the server. Use of server alive messages is very different from TCPKeepAlive (below). Server alive messages are sent through the encrypted channel and therefore will not be spoofable. The server alive mechanism is valuable when the client or server depend on knowing when a connection has become inactive. See **ssh_config** man page, key word *ServerAliveCountMax*.
[ResponseTimeOut]	120	The time allowed for process client response.
[Debug]	0	Possible values are 0 (disable debug mode) and 1 (enable). If you enable debug mode, modify *syslog.conf* file to set an entry as follows: 1.Set an entry as below for ServerProtect in syslogd's configuration file, /etc/syslog.conf. In ***/etc/syslog.conf***: #Save boot messages also to boot. loglocal7.* ***/var/log/boot.log*** local6.* [where you want to put your debug log] <- add this line 2.Find syslogd's pid. (pidof syslogd) 3.Set syslogd to reread its configuration: (`kill –HUP `pidof syslogd``)
[StatusFile]	splx_remote_status	Indicates the file name for deployment status.
[FullStatus]*	disabled	Records detailed deployment status in the StatusFile.
[SuccessList]	splx_success_list	Indicates the file name for list of clients for which deployment succeeded.
[FailedList]	splx_failed_list	Indicates the file name for list of clients for which deployment failed.

* Trend Micro recommends that you keep this default value

TABLE A-4. `RemoteInstall.conf` **keys, default values, and descriptions**

Using `splxmain`

The `splxmain` command enables you to maintain and control ServerProtect from the command line. Use `splxmain` for various ServerProtect maintenance tasks that are run through cron(8) or crond(8) or that can be run from the command line. You must have root (superuser) privileges to run splxmain.

Note: You should only use `splxmain` to run ServerProtect without Apache.

`splxmain` controls the processes ServerProtect uses for scanning, logging, updating, and so on.

Location:

`/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp/splxmain`

Syntax:

```
splxmain [-a |-b |-c | -De |-E |-f |-g <date> |-i |-j |-k
|-l <port> |-m [path1:path2] |-n |-o |-p |-q <Activation Code>
|-r |-s |-t |-u |-v |-w <port> |-x |-y ]
```

Note: Except for ***-D***, specify only one parameter at a time.

Parameters:

`-a` Terminate all vsapiapp processes, Manual Scan processes, and Scheduled Scan processes gracefully. To terminate these processes immediately, use the -k option.

`-b` Remove all scheduled jobs from the `/etc/cron.d/splx` file. file, letting currently running jobs complete.

`-c` Refresh the Scheduled Scan, Scheduled Update, and Scheduled Log purging settings based on the settings in the tmsplx.xml file to `/etc/cron.d/splx` file.

`-D` Force vsapiapp to run as a daemon. Use this option with `-e`.

`-e` Read the tmsplx.xml(5) configuration file and set up the `/etc/cron.d/splx` tables to run Scheduled Scans, Scheduled

Updates, and Automatic Log Purges, then launch vsapiapp. If the `-D` option is also specified, vsapiapp is run as a daemon; otherwise, it is run as a regular process. -D can be used with this option.

Note: If `-D` is used in conjunction with `-e`, vsappiapp runs as a daemon; otherwise, it runs as a regular process.

`-E` Check the remaining days left before the evaluation version expires.

`-f` Reset the Web console password to the default value of null. If you forget the Web console password, you can use this option to reset it to null and then use the `-j` option to assign a new password.

`-g <date>` Purge ServerProtect log files. The `<date>` is an actual cut-off date specified in YYYY-MM-DD format. For example:

```
splxmain -g 2006-04-21 # deletes logs written before April 21, 2006
```

Note: If you do not specify `<date>`, ServerProtect will use the value of the `MaxLogDay` key in the `tmsplx.xml` file. See *MaxLogDay* on page A-26.

`-i` Restart the vsapiapp processes.

`-j` Set the Web console password. Type the new password twice for confirmation.

`-k` Terminate the vsapiapp processes, manual scan processes, and scheduled scan processes immediately by sending a `SIGKILL` signal. To terminate these processes gracefully, use the `-a` option.

`-l <port>` Set the ServerProtect HTTP port for accessing the ServerProtect Web console.
For example, `splxmain -l xxxxx`

`-m <directory>` Execute a Manual Scan based on the Manual Scan settings in the `tmsplx.xml` file. Use a colon (:) to separate multiple directories. For example, to scan `/temp1` and `/temp2`:

```
splxmain -m /temp1:/temp2
```

Note: Executing a manual scan does not require running or triggering the KHM.

`-n` Terminate the manual scan process that is currently running.

`-o` Remove the scheduled scan processes from the `/etc/cron.d/splx` file.

`-p` Trigger the Scheduled Update process.

Note: The exact update time is written into `/etc/cron.d/splx` when ServerProtect service is first started. When you launch a scheduled update, the update time is modified. Use the `./etc/cron.d/splx -l` command to list all scheduled tasks.

`-q <Activation Code/serial number>` sets the Activation Code/serial number.

`-r` Reload the ServerProtect configuration without restarting vsapiapp.

`-s` Execute Scheduled Scan now. Usually, the `-m` option is used to run an on-demand scan. However, this option is used in `/etc/cron.d/splx` and can be used to run an on-demand scan with the settings specified for a Scheduled Scan specified in the `tmsplx.xml` file.

Note: Executing a scheduled scan does not require running or triggering the KHM.

`-t` Terminate the Scheduled Scan processes that are running through cron or crond. `/etc/cron.d/splx.`

`-u` Update the scan engine and virus pattern according to `tmsplx.xml` and ask vsapiapp to reload these components.

`-v` Enable real-time scan by spawning child threads for real-time scan.

`-w <port>` Set the HTTPS port for accessing the ServerProtect Web console. For example:

```
splxmain -w 12345
```

`-x` Disable real-time scan by terminating the real-time scan child threads.

`-y` Set the user name and password for the proxy server used for component download.

This information is also available in the splxmain man page, which you can access from the command line by issuing this command:

```
# man splxmain
```

Using `splx` Script

Use **splx** script to enable/disable ServerProtect.

Location:

```
/etc/init.d/
```

Syntax:

```
splx {start|stop|restart|status}
```

Parameters:

`start`

Starts the ServerProtect service and the ServerProtect Apache server

`stop`

Stops the ServerProtect service and the ServerProtect Apache server

`restart`

Stops, and then restarts the ServerProtect service and the ServerProtect Apache server

`status`

This parameter displays all active ServerProtect core services and the TMCM-registration status.

Using `splxcore` Script

Use the **splxcore** script to run ServerProtect without the Apache server.

Note: Use the splxcore script to manage ServerProtect from the command line (no Web console). Some features, such as product registration after ServerProtect is installed or log query, are not available from the command line.

Location:

```
/etc/init.d/
```

Syntax:

```
splxcore {start|stop|restart|status}
```

Parameters:

`start`

Starts the ServerProtect core service

`stop`

Stops the ServerProtect core service

`restart`

Stops, and then restarts the ServerProtect core service

`status`

Displays currently active ServerProtect core processes

Using `splxhttpd` Script

Use the **splxhttpd** script to enable/disable the Apache server.

Location:

```
/etc/init.d/
```

Syntax:

```
splxhttpd {start|stop|restart|status}
```

Parameters:

`start`

Starts ServerProtect Apache server

`stop`

Stops the ServerProtect Apache server

`restart`

Stops, and then restarts the ServerProtect Apache server

`status`

Displays currently active ServerProtect Apache processes

Using `splxcomp` Script

This tool is designed to avoid redundant scanning when installing Trend Micro InterScan VirusWall for Linux and ServerProtect on the same server. Use `splxcomp` to locate and exclude InterScan VirusWall for Linux quarantine and backup directories. It resides in this folder:

```
/opt/TrendMicro/SProtectLinux/SPLX.util/
```

`splxcomp` prevents redundant scanning when installing Trend Micro InterScan™ VirusWall™ for Linux and ServerProtect on the same server. Use `splxcomp` to locate and exclude InterScan VirusWall for Linux quarantine and backup directories.

Note: Use this tool only when installing InterScan VirusWall for Linux and ServerProtect on the same server.

Syntax:

```
splxcomp {-h} {-v} {-i}
```

Parameters:

`-h` displays the tool's parameters list

`-v` displays version information

`-i` obtains critical settings from Trend Micro InterScan VirusWall

Using the `CMconfig` Tool

You can use to `CMconfig` to register ServerProtect to and unregister it from Trend Micro Control Manager (TMCM).

The CMconfig utility senses whether or not ServerProtect is registered to TMCM. CMconfig acts as a toggle switch: if ServerProtect is currently registered to TMCM, CMconfig unregisters it; if not, CMconfig registers ServerProtect to TMCM.

Location:

```
/opt/TrendMicro/SProtectLinux/SPLX.util
```

Syntax:

```
./CMconfig
```

Parameters:

(none)

Apache Configuration File

ServerProtect uses its own customized Apache server. Its configuration file can be found on the following path:

`/opt/TrendMicro/SProtectLinux/SPLX.httpd/conf/splxhttpd.conf`

WARNING! *Editing the customized Apache server configuration file may result in unexpected errors. Before making any changes to this file, back up* `splxhttpd.conf` *to restore your original settings. Contact Trend Micro Support for help when editing* `splxhttpd.conf`.

Apache Log Files

You can find ServerProtect Apache server log files in the following directory:

`/opt/TrendMicro/SProtectLinux/SPLX.httpd/logs/`

SMTP Mail Notification Character Sets

The following is a sampling of the character sets that ServerProtect supports. For information on how these character sets are use, see *To enable SMTP mail notification:* on page 4-28.

Character Set	What you should type in the Charset field
English	us-ascii
Japanese	iso-2022-jp
Latin 1 Western European (default)	iso-8859-1
Korean	euc-kr
Traditional Chinese	big5
Simplified Chinese	gb2312

TABLE A-5. SMTP mail notification character sets

Debian Commands

The following Debian-specific commands may be used in ServerProtect 2.5 for Linux:

Command	Description
`sh Sprotect~.bin`	Install new version
`dpkg`	Package manager
`dpkg -i install~.deb`	Upgrade to newer version
`dpkg --purge sprotectlinux`	Remove ServerProtect. The tmsplt.xml file is backed up with the file extension "dpkg-save."
`dpkg -r sprotectlinux`	Remove ServerProtect, retain configuration files and system initial services
`rcconf`	Configure start-up settings using the terminal only

TABLE A-6. ServerProtect 2.5 Debian-specific commands, described

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

Term	Explanation
?	Character that can be used as a wildcard when specifying directories to be scanned or excluded from scanning.
access (verb)	To read data from or write data to a storage device, such as a computer or server.
access (noun)	Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.
action	The operation to be performed when a virus or other malware has been detected. Actions typically include clean, quarantine, delete, or pass (deliver/transfer anyway). Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your software after completion of the registration process. Trend Micro products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the Product License screen.

Term	Explanation
Activation Code	A 24-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: 9UE7-HG53-857B-TD54-MMP8 *Also see* Registration Key.
ActiveAction	A set of preconfigured actions (such as clean, delete, or quarantine) to be performed on files that have been affected by a security risk, such as a virus, Trojan, spyware/grayware, or joke program.
ActiveUpdate	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files via the Internet or the Trend Micro Total Solution CD.
administrator account	A user name and password that has administrator-level privileges.
alert	A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition.
Big 5	A character encoding method used in Taiwan and Hong Kong for encoding traditional Chinese characters. Refer to the following Web site for more information: http://en.wikipedia.org/wiki/Big5
clean	To remove virus code from a file or message.
CMconfig	A ServerProtect 2.5 utility that you can run from the command line to register SeverProtect to Trend Micro Control Manager, to unregister it, or to re-register it.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
damage routine	The destructive portion of virus code, also called the payload.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.

Term	Explanation
ELF	Executable and Linkable Format—An executable file format for Unix and Linux platforms.
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.
EUC-KR	A method of 8-bit character encoding used for the Korean language. See the following Web site for more information: *http://en.wikipedia.org/wiki/EUC-KR*
EXE file infector	An executable program will a .exe file extension. *Also see* DOS virus.
exploit	An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.
failover	The process of automatically switching to a redundant server, system, or network in case your currently active component fails. Failover systems are employed when a critical service, such as ActiveUpdate, is needed on a continuous basis.
file-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.

Term	Explanation
gateway	An interface between an information source and a Web server.
GB 2312	A method of character encoding used for Simplified Chinese characters in mainland China and Singapore. See the following Web site for more information: *http://en.wikipedia.org/wiki/Guobiao_code*
grayware	A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
header (networking definition)	Part of a data packet that contains transparent information about the file or the transmission.
HTML virus	A virus targeted at HTML (Hyper Text Markup Language), the authoring language used to create information in a Web page. The virus resides in a Web page and downloads via a user's browser.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
host	A computer connected to a network.
incoming files	Files being placed on your server.
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition, and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.
"in the wild"	Describes known viruses that are actively circulating. *Also see* "in the zoo."
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—*See* IP address.

Term	Explanation
IP address	Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.
ISO-2002-JP	A widely-used character encoding method for the Japanese language See the following Web site for more information: http://en.wikipedia.org/wiki/ISO_2022
ISO-8859-1	A character encoding language that uses a single 8-bit code to represent an alphabetic character. ISO-8859-1 supports many European languages. See the following Web site for more information: *http://en.wikipedia.org/wiki/Iso-8859-1*
Java Runtime Environment (JRE) 	A Java Virtual Machine, set of class libraries, and other components needed to run applets and applications written in the Java programming language. The JRE also includes a Java plug-in and Java Web Start, which enables you to launch Java-based applications without complicated installation procedures. Refer to the following Web site for more information: *http://java.sun.com*
joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system.
Konquerer Desktop Environment (KDE) 3.2 	The KDE is a easy-to-use desktop environment for Unix platforms, that offers an integrated help system, a consistent look and feel for applications, standardized menus and toolbars, internationalization, and useful applications. KDE version 3.2 is required for use of the Quick Access console menus in ServerProtect. For more information about KDE, refer to the following Web site: *http://www.kde.org/*
Kernel Hook Module (KHM)	A linking mechanism between ServerProtect and your version of the LInux operating system.
Latin-1	One of 6 preferred character sets available with ServerProtect. *Also see* ISO-8859-1.
license certificate	A document that proves you are an authorized user of a Trend Micro product.
listening port	A port utilized for client connection requests for data exchange.

Term	Explanation
load balancing	Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.
log storage directory	Directory on your server that stores log files.
macro	A command used to automate certain functions within an application.
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. Macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
macro virus	Macro viruses are often encoded as an application macro and included in a document. Unlike other virus types, macro viruses are not specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.
management console	The user interface for your Trend Micro product.
mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
multi-partite virus	A virus that has characteristics of both boot sector viruses and file-infecting viruses.
network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.

Term	Explanation
Novell Linux Desktop 	A GNU/Linux distribution from Novell, Inc, based off of SUSE 9 Enterprise Server technology. For more infomation, see the following Web site: *http://www.novell.com/*
outgoing files	Files being copied or moved from your server to another location.
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
polymorphic virus	A virus that is capable of taking different forms.
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
quarantine	To place infected data such as infected HTTP downloads or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
Quick Access console	Menus and ServerProtect command-line equivalents installed in the KDE.
Red Hat 	An open source operating system produced by Red Hat, Inc. For more information, see the following Web site: *http://www.redhat.com/*
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8
RemoteInstall	A ServerProtect 2.5 utility that can be used to to install ServerProtect on remote machines, to update the KHM on remote machines, to convert .CSV result files into RemoteInstall.conf format, and to update ServerProtect 2.5 configuration on remote machines.
RemoteInstall.conf	The config file for the RemoteInstall utility

Term	Explanation
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.
Samba 	Samba is an open source suite of software that provides file and print services which allow a host running on a non-Windows platform to interact with a Windows client or server as if it were a Windows file and print server. For more information, see the following URL: *http://us5.samba.org/samba/*
sector	A physical portion of a disk. (*Also see* partition, which is a logical portion of a disk.)
Secure Sockets Layer (SSL)	Secure Sockets Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
signature	*See* virus signature.
Simplified Chinese	One of 6 preferred character sets available with ServerProtect. *Also see* GB 2312.
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
squid	An open source proxy server and Web cache.
SUSE 	An open source operating system produced by Novell, Inc. For more information, see the following Web site: *http://www.novell.com/*
TCP	Transmission Control Protocol—TCP is a networking protocol, most commonly used in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.

Term	Explanation
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.
Total Solution CD	A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD is available to all Trend Micro Premium Support customers.
Traditional Chinese	One of 6 preferred character sets available with ServerProtect. *Also see* Big 5.
trigger	An event that causes an action to take place. For example, your Trend Micro product detects a virus in an email message. This may *trigger* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan Horse	A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.
true file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
US-ASCII	A character encoding method used in modern English and other Western European languages. See the following Web site for more information: *http://en.wikipedia.org/wiki/US-ASCII*
VBscript virus	VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a Web page. A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser. *Also see* JavaScript virus.

Term	Explanation
virus signature	A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.
virus writer	Another name for a computer hacker, someone who writes virus code.
wildcard	A term used in reference to specifying a directory path, where an asterisk (*) represents any characters. For example, to specify any directory 2 levels down from /opt, you could type /opt/*/*. The term originates from card games, in which a specific card, identified as a "wildcard," can be used for any number or suit in the card deck.
worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.
"Zip of Death"	A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X