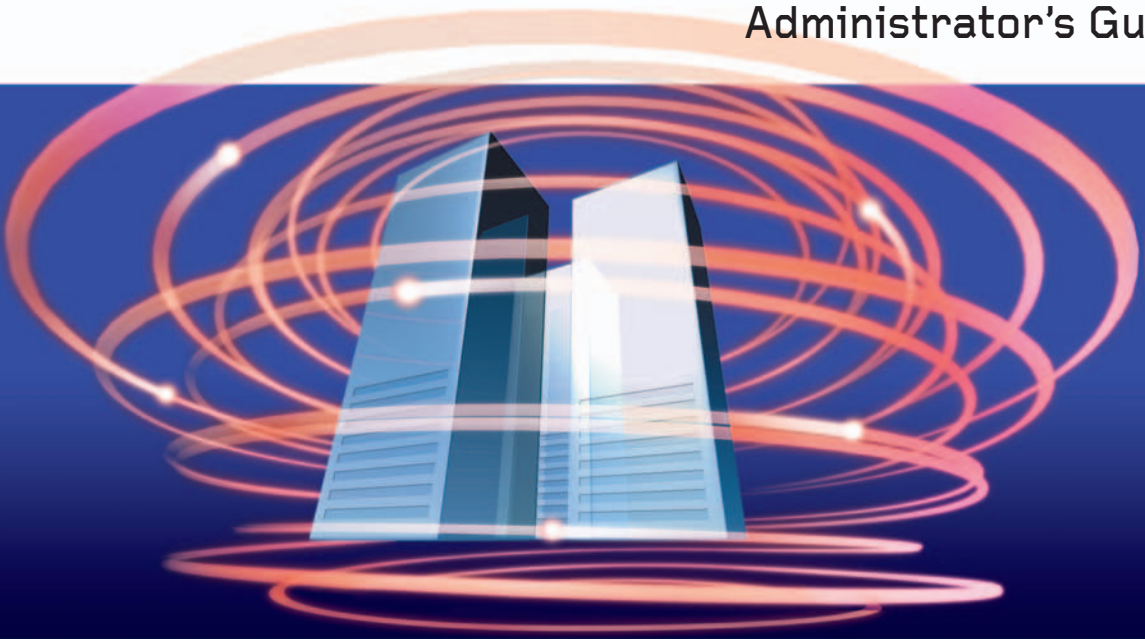# TREND MICRO™
ServerProtect™ 3

Centrally managed virus protection for enterprise-class servers and storage systems

for LINUX™

Administrator's Guide

TREND MICRO™

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

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro™ ServerProtect™ collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

v

Contents

i

Chapter 3: Configuring and Performing Scans with ServerProtect

Chapter 4: Update

Chapter 5: Logs

Index

Appendix 1: Glossary of Terms

Preface

Welcome to the Trend Micro™ ServerProtect™ for Linux 3.0 (SPLX3.0) Administrator's Guide for release 3.0. This guide provides detailed information about configuration options for ServerProtect for Linux.

Topics include basic information about the tasks you need to perform to install the product and basic configuration. This preface discusses the following topics:

ServerProtect Documentation

The Trend Micro™ ServerProtect™ for Linux 3.0 for release 3.0 documentation consists of the following:

- It also includes instructions on testing your installation using a harmless test virus.

- **Online help**—The online help provides "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.

- **Linux Man pages**—ServerProtect for Linux provides man pages for the `splxmain`, `splx`, `tmsplx.xml`, `RemoteInstall`, and `CMconfig`. See *Accessing ServerProtect Man Pages* starting on page B-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/`

Tip: Trend Micro recommends checking the corresponding link from the Update Center (`http://www.trendmicro.com/download`) for updates to the product documentation.

Audience

The Trend Micro™ ServerProtect™ for Linux 3.0 documentation assumes an intermediate to advanced knowledge of Linux system administration, including:

- Installing and configuring Linux servers
- Installing software on Linux servers
- Network concepts (such as IP address, netmask, topology, LAN settings)
- Various network topologies
- Network devices and their administration
- Network configuration (such as the use of VLAN, SNMP, SMTP)

Document Conventions

To help you locate and interpret information easily, the documentation uses the following conventions.

Convention	Description
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

TABLE P-1.   Conventions used in the documentation

Chapter 1

Introduction

Managed through an intuitive portable Web-based console, ServerProtect provides centralized virus/malware scanning, pattern updates, event reporting, and antivirus configuration.

This chapter discusses the following topics:

The Problem

While Linux systems are less vulnerable than Windows systems, they are not immune. Many Linux systems are used as file servers for Windows systems. Without protection against viruses/malware and other security risks at the server level, Windows threats may quickly spread across the network.

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.

A solution is required that can:

- Scan and effectively detect viruses/malware, worms, Trojans, and spyware/grayware on Linux systems.
- Perform appropriate actions on the suspicious files.
- Provide notification to administrators.

The ServerProtect for Linux Solution

ServerProtect for Linux scans data and executable files on Linux systems to detect and protect against viruses/malware, worms, Trojans, and spyware/grayware.

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.

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 unscannable). The administrator can designate all such files for automatic quarantine or choose to have the scan engine ignore these files.

Platforms That Can Scan

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

Scripting Languages

- JavaScript
- VBScript

Main Features

The following are main features of ServerProtect for Linux:

Manage ServerProtect with Trend Micro Control Manager™

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 Control Manager 3.5. When registered to Control Manager, ServerProtect can make use of Control Manager features such as

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

Reports Available from Control Manager

The following reports are available from Control Manager:

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

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

Multiple-Processor Support

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

Remote Management Through a Web Browser

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

Manual, Real-Time, and Scheduled Scanning

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

Application Execution Protection

ServerProtect's Real-time Scan option also detects viruses/malware in Linux applications whenever an application is executed. See *Exclusion List* on page 3-14 for additional information.

Backup Directory Configuration

This is useful when an infected file cannot be cleaned and as a result it is not recoverable.

Detailed, Easy-to-Maintain and Exportable 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. You can also export comprehensive logs about system and/or antivirus activities performed on your system.

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.

Notification of Virus Outbreaks

You can configure about events, such as virus/malware 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/malware 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/malware outbreaks, minimize system damage, and prevent undue downtime.

When registered to 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 OPS 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`.

Award-Winning Software

ServerProtect is a proven award-winning product.

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, log deletions, and virus pattern/engine updates. See Appendix A, *Using splxmain* starting on page B-37, for information about command line options.

Support for Advanced ActiveUpdate Options

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 HTTPS and SSL)
- Squid with digest authentication (both HTTPS and SSL)

Consistency Checking Between ServerProtect 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 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 an Activation Code on the Trend Micro Registration Web site:

```
https://olr.trendmicro.com/redirect/product_register.aspx
```

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 *Debug Logging* on page 6-3 for details.

Safer Configuration File Modifications

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.

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.

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.

Support for Multiple Update Sources

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.

HTTPS (SSL) Support

You can access the ServerProtect Web-based console using the HTTPS protocol. See *Accessing the ServerProtect Web Console* on page 2-2 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 Console for X Window System

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
- Display the notification icon in the system tray

An Improved User Interface

If you are familiar with previous versions of ServerProtect, you may notice that the look and feel in this version is slightly different from the previous version. The appearance have changed, and the overall design of the user interface has been enhanced. For example:

Enhanced links available from drop-down menu

Launch context-sensitive help from here

FIGURE 1-1.   Enhanced user interface

Remote Installation

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

One Binary Package for All Supported Linux Distributions

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

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.

What's New in This Release

For customers who are familiar with previous versions of Server Protect for Linux, the following new features are available in version 3.0:

Support for 64-bit Processors

ServerProtect is designed to take advantage of the enhanced speed and efficiency provided by AMD64/EM64T processors.

Note: This version of ServerProtect does not support IA64bit processors.

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 4.0 (AS, ES, WS, and Desktop)
- Red Hat™ Enterprise Linux 4.0 for AMD64/EM64T (AS, ES, WS, and Desktop)
- Red Hat™ Enterprise Linux 5.0 (Server and Desktop)
- Red Hat™ Enterprise Linux 5.0 for AMD64/EM64T (Server and Desktop)
- SUSE™ Linux Enterprise Server 10 (Server and Desktop)
- SUSE™ Linux Enterprise Server 10 for AMD64/EM64T (Server and Desktop)

GPL Open Source KHM

By going open source, Trend Micro provides the flexibility that allows you to recompile KHM for your Linux kernel. Useful readme documents, test scripts and makefiles are provided to guide you through the build process.

Logon Session Control

For better security, the Web console session control feature is included. This allows the ServerProtect Web console to automatically log you out (terminates the session) after 20 minutes (1200 seconds) of inactivity.

Summary Page

You can display the new Summary screen to monitor your Linux system's protection against viruses/malware. You can view information such as the system status, scan results/status, and update status.

World Virus Tracking Program (WVTP)

Trend Micro's World Virus Tracking Program collects Internet threat data from tens of thousands of corporate and individual computer systems around the world.

Anti-spyware

Trend Micro's Anti-spyware technology is designed to block spyware/grayware and adware, plus hacking and remote access tools that could harm the network. This added security helps prevent intruders from collecting personal or corporate information, passwords, email addresses, and other data. It also frees system resources and available bandwidth, improving network performance and reducing spyware-associated system failures.

Notification Icon and Pop-up Virus Information

When you use the graphical KDE on your Linux system, the ServerProtect Notification icon automatically displays in the system tray to provide real-time scanning status. When ServerProtect detects a virus/malware, the Notification icon changes. Double-click on the icon to display detailed information about the virus/malware in a pop-up window.

SMTP Authentication

You can enable SMTP authentication for sending email notifications.

Bypass Password for Local Logon

You can bypass password checking when logging on to the same server where you installed ServerProtect.

Option To Exclude OpenAFS Network Drives From Scanning

You may have network file systems that you want to exclude from scanning. In addition to popular mapped drive format, now you can also exclude OpenAFS mapped drives from manual and scheduled scanning.

Understanding How ServerProtect 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.
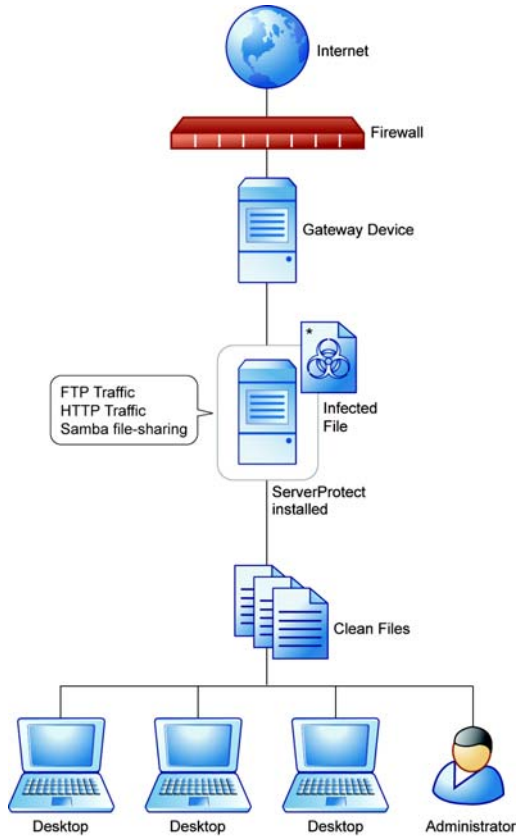
FIGURE 1-2.   How ServerProtect works

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 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/malware, 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. Compressed files bypassing a scan action appear in the system logs. It is important to note that the smaller the size specified, the higher the risk of infection.

Note: During a decompression attempt, Real-time Scan will still detect viruses in compressed files that ServerProtect has skipped scanning.

Getting Started with ServerProtect

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

This chapter discusses the following topics:

Accessing 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.

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.

You can access the Web console using one of the following:

- Quick Access console in KDE
- Trend Micro ServerProtect for Linux icon
- A supported Web browser

To access the Web console:

1. Log on as *root*.
2. Do one of the following:
    - In KDE, click **Start Applications Menu** > **System (Tools) > Trend Micro ServerProtect> Launch Web Console**.
    - Double-click the Trend Micro ServerProtect for Linux icon on the KDE or GNOME desktop.
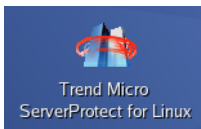
FIGURE 2-1.   ServerProtect desktop icon

- In a supported web browser, type the location of the ServerProtect computer and the port number in the address field:

    ```
    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 the `splxmain` command. See *Using splxmain* starting on page B-37 for more information.
If you are using Internet Explorer 7.0, you must disable pop-up window blocker to display the online help content.

---

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

Setting Logon Password

For protection, change the Web console password after logging on for the first time.

To configure logon password:

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 be between 0 and 32 characters, and should only contain alphanumeric characters (A-Z, a-z, 0-9) and characters such as hyphen (-).
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.

Bypassing Password Checking for Local Logon

You can disable password checking during logon when you are logging on the same server you installed ServerProtect.

To bypass logon password:

1. Select **Administration** > **Password** from the left menu on the Web console.
2. Select **Bypass password when logging on**.

3. Click **Save**.

Note: When logging on from another computer or using a secure proxy from the machine-installed ServerProtect for Linux, you still need to type the password to log on.

Logging off from the Web Console

To log off from the console, click [Logout] on the title bar.

Things to Remember About the 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 (refer to *Starting and Stopping ServerProtect* on page 2-7).

- To refresh a Web console screen, use your browser's Refresh option.

- The Web console automatically logs you out after 1200 seconds (or 20 minutes) of inactivity. If this happens to you, type the password and click **Logon** to access the Web console again. You can change the default timeout settings by changing the `SessionTimeout` key in the `Configuration` section in the `tmsplx.xml` file (located in the `/opt/TrendMicro/SProtectLinux` folder).

  The session control feature does not apply to the following:

  - local logon bypassing password checking
  - access the ServerProtect Web console via Single Sign On (SSO) using Control Manager

Using the Quick Access Console Menus

When you have KDE version 3.3 (or above) installed on the ServerProtect computer, the installation program adds the Trend Micro ServerProtect menu option to your desktop in one of the following places:

- System Menu (SUSE)
- System Tools Menu (Red Hat)

Note: Accessing the Quick Access console requires logging on as the *root* user.
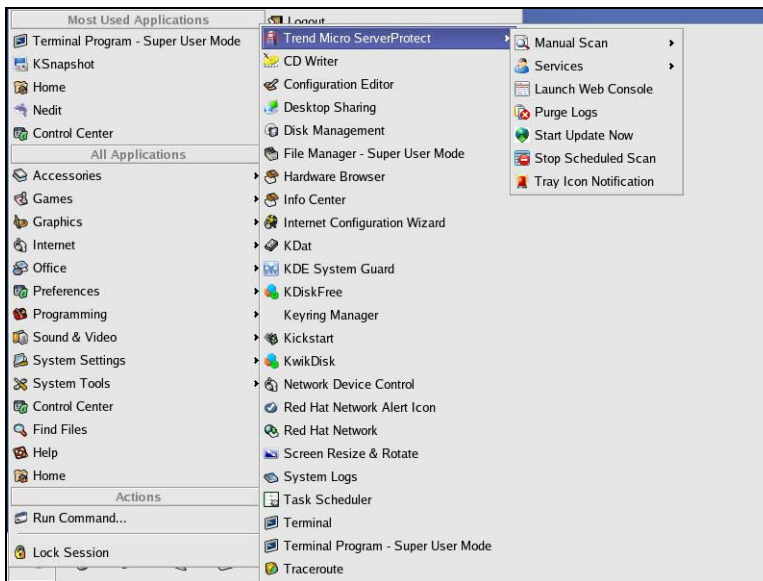
FIGURE 2-2.   Quick Access Console Menu in KDE

The following describes the menus/options available:

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

2-5

- **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, spyware/grayware, 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
- **Tray Icon Notification**—This option displays the ServerProtect notification icon in the system tray

Starting and Stopping ServerProtect

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

There are two ways to start or stop ServerProtect:

•   From the command line

•   From the Quick Access console

Note: By default, ServerProtect starts whenever you turn on the server hosting it. To change this setting, see *Configuring Startup Settings* on page 2-9.

Starting ServerProtect

To start ServerProtect from the command line:

1.   Log on as *root*.

2.   Open a terminal screen and type /etc/init.d/splx start in the command line. The following messages appear.

```
[root@localhost ~]# /etc/init.d/splx start
Starting ServerProtect for Linux:
Checking configuration file:                          [  OK  ]
Starting splxcore:
Starting Entity:                                      [  OK  ]
Loading splx kernel module:                           [  OK  ]
Starting vsapiapp:                                    [  OK  ]
ServerProtect for Linux core started.
                                                      [  OK  ]
Starting splxhttpd:
Starting splxhttpd:                                   [  OK  ]
ServerProtect for Linux httpd started.
                                                      [  OK  ]
ServerProtect for Linux started.
[root@localhost ~]#
```

To start ServerProtect from the Quick Access console:

1.   Log on as *root*.

2.   From the task bar, click **Start Applications Menu** > **System (Tools)** > **Trend Micro ServerProtect** > **Services** > **Start SPLX Service**.

Stopping ServerProtect

To stop ServerProtect from the command line:

1. Log on as *root*.

2. Open a terminal screen and type `/etc/init.d/splx stop` in the command line. The following messages appear.

```
[root@localhost ~]# /etc/init.d/splx stop
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.
[root@localhost ~]#
```

To stop ServerProtect from the Quick Access console:

1. Log on as *root*.

2. From the task bar, click **Start Applications Menu** > **System (Tools)** > **Trend Micro ServerProtect** > **Services** > **Stop SPLX Service**.

Notification Icon

The notification icon in the system tray indicates the status of ServerProtect service on your Linux computer and also alerts you when a virus/spyware is detected.

The following table describes the notification icon status.

Icon	Description
	ServerProtect is running properly.
	ServerProtect is not running.
	ServerProtect has detected a virus/spyware on your Linux computer. Until you double-click on this icon to display the virus information screen, ServerProtect continues to display this warning icon in the system tray even when the Server-Protect service has stopped running.

TABLE 2-1.   Notification icon

Note: By default, the notification icon displays in the KDE system tray for the root user only. To display the notification icon in the KDE system tray for other users, set the access rights for the `/opt/TrendMicro/SProtectLinux/SPLX.tmp` directory and the `virus_catch_monitor` file in `/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp`.

Notification Information Screen

The notification information screen displays real-time virus/spyware detection information. To display this screen, double-click on the notification icon in the system tray.

Information for the scan result include:

- Name of the virus/spyware
- Name of the infected file
- Action(s) performed
- Date and time detected

Note: The notification information screen displays up to the latest 50 virus/spyware logs. When you close the notification information screen, ServerProtect automatically clears the virus/spyware logs in this screen. To view the virus/spyware logs again, open the corresponding Log screens in the ServerProtect Web console.

Configuring Startup Settings

By default, ServerProtect starts whenever you turn on the server hosting it. To change the startup setting, use the Linux Service Configuration utility. The method of configuring startup settings varies for each supported Linux distribution.

To display help information on startup settings in the ServerProtect Web console, select **Administration > Startup Settings** and click the **system administration tool** link. The following screen appears:

FIGURE 2-3.   Administration: Startup Settings

Red Hat™ Enterprise Linux 4

Using the Service Configuration utility:

1. Log on as *root* and type `system-config-services` in the command line. The Service Configuration utility screen appears.

2. Select **Edit Runlevel** on the menu and then choose level 3, 4, or 5 to edit.

3. Scroll down the screen and select **splx**.
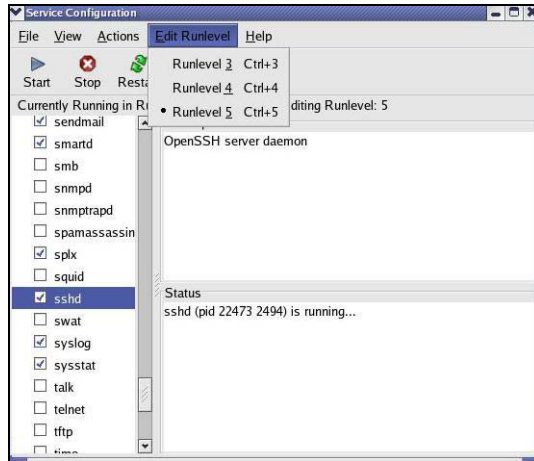
FIGURE **2-4.** **Red Hat: Service Configuration Utility**

4. To start the service manually, do not select **splx** on level 3, 4, or 5.

Using the Text Mode Setup utility:

1. Log on as *root* and type `setup` in the command line. The Text Mode Setup Utility screen appears.

2. Press the arrow key to select **System services**, then press [ENTER].
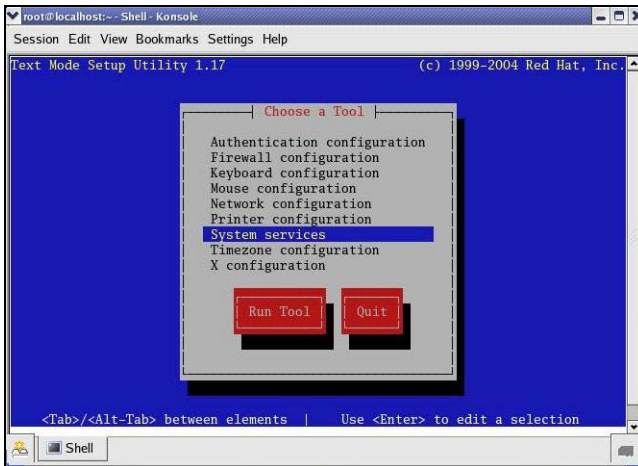
FIGURE 2-5.   Red Hat: Text Mode Setup Utility

3. Select **splx** to configure ServerProtect to start automatically. Clear the **splx** check box to start manually.

SUSE Linux Enterprise Server

Using the graphical screen:

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, 4, or 5. To start the service manually, do not select a level.

Using the terminal:

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, 4, or 5. To start the service manually, do not select a level.

Viewing Summary Information

The **Summary** screen provides current system versions, an overview of network virus scan results, and existing Trend Micro antivirus component details.

From the **Summary** screen, you can:

- View system information including the operating system and hardware versions.
- View scan results for viruses/spyware.
    - The **viruses/spyware detected today** field displays the total number of viruses/spyware detected during the past 24 hours.
    - The **Today** field displays the number of viruses/spyware ServerProtect detects and performs the specified actions upon for the last 24 hours.
    - The **Last 7 days field** displays the total number of viruses/spyware detected for the last seven days (including the current day).

Note: ServerProtect may perform more than one action on a detected virus/spyware, thus the virus/spyware is counted in more than one **Summary** field.
The MaxRetrieveCount parameter in the tmsplx.xml file specifies the maximum number a counter can display. Refer to *MaxRetrieveCount* on page B-29 for more information.

- View scan status and click **Scan Now** to perform on-demand scanning.
- View component status and click **Update Now** to update the selected components.

Managing ServerProtect From Control Manager

To benefit from the information the ServerProtect server can provide, you must register the ServerProtect server to Control Manager. ServerProtect communicates to Control Manager through the Trend Micro Management Communication Protocol (MCP) agent. The MCP agent is installed with the computer on which ServerProtect is installed, so there is no need for you to install the MCP agent.

You can register ServerProtect to Control Manager using one of the following methods:

- During the installation process
- ServerProtect Web console
- The command line using the CMconfig tool

To register ServerProtect to Control Manager using the Web console:

1. Log on to the Web console.

2. Click **Administration > Control Manager Settings**. The **Control Manager Settings** screen displays.

FIGURE 2-6.   Control Manager

3. Under **Connection Settings**, configure the following fields:

- Type the name of the ServerProtect computer in the **Entity display name** field. Choose this name carefully because this is the name that will display on the Control Manager server Product Directory to identify the ServerProtect server. A unique and meaningful name will help you to quickly identify the ServerProtect server in the Product Directory of Control Manager.

- In the **Group folder name** field, type a descriptive name that identifies ServerProtect in the Control Manager product tree.

- In the **Server name or IP address** field, type the host name or the IP address of the computer on which you installed ServerProtect. Trend Micro recommends typing the server name if you have configured DNS settings for your network environment.

4. Under **Control Manager Server Settings**, specify the following:

   a. Type the Control Manager server IP address or host name in the **Server name or IP address** field.

   b. Type the port number that the MCP agent uses to communicate with Control Manager.

   c. If you have Control Manager security set to medium (HTTPS and HTTP communication is allowed between Control Manager and the MCP agent of managed products) or high (Only HTTPS communication is allowed between Control Manager and the MCP agent of any managed products), select **Connect using HTTPS**.

   d. If your network requires authentication, type the user name and password for your Internet Information Services (IIS) server in the **User name** and **Password** fields.

Note: If you use IIS server authentication, you cannot set ServerProtect to update components from Control Manager. You must specify the URL of an update server (either the official Trend Micro update server or the one you set up) as the download source in the **Scheduled Update** or **Manual Update** screen.

---

   e. If you use a proxy server to access the Internet, specify the proxy server settings under **Proxy Settings**.

     f.   If you use a NAT device, clear the **Enable two-way communication** check box.

5. Click **Register** to save the settings and register the ServerProtect computer to Control Manager.

To register ServerProtect to Control Manager using the CMconfig tool:

1. If you have verified that ServerProtect is currently not registered to Control Manager, execute the CMconfig utility. Type the following command in the `/opt/TrendMicro/SProtectLinux/SPLX.util` directory.

    `./CMconfig`

2. ServerProtect prompts you for necessary data and displays a list of available IP addresses for your ServerProtect server.

Note: For details on command options, type `./CMconfig -h` at the command line. To specify a proxy type, change the `Proxy_Type` parameter in the `Agent.ini` file (located in the `/opt/TrendMicro/SProtectLinux/` folder) before you use the `CMconfig` command to register ServerProtect to Control Manager.

---

3. At the `SPLX server name or IP address:` prompt, enter the name or IP address of your ServerProtect server.

4. At the `Do you wish to connect to Control Manager server using HTTPS? (y/n) [n]` prompt, type y to connect to Control Manager using HHTPS; otherwise type n to use HTTP connection.

5. At the `Control Manager server name or IP address:` prompt, enter the name or IP address of the Control Manager server that you want to use to manage ServerProtect.

6. At the `Control Manager server port: [80]` prompt, 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.

7. At the `Do you access Control Manager through a proxy server? (y/n) [n]` prompt, type y and press Enter if you do or just press Enter to accept the default choice of n. If you choose n, CMconfig prompts you to specify the display name to identify ServerProtect on the Control Manager Web console.

Tip: If you use a proxy server to connect to Control Manager, see "Entering Proxy Server Information" in the Installation chapter of the Getting Started Guide for further guidance on this process.

---

8. 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.

9. At the `Please specify a folder name for this product (for example: /SPLX) [New entity]:` prompt, enter the folder path described above. CMconfig displays a summary of the information you have entered and asks you to confirm your choices.

10. At the `Is the above information correct? (y/n) [n]` prompt, confirm or reject the displayed choices. If you type n (or just press Enter to accept the default choice of n), CMconfig 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, CMconfig outputs status messages as it registers ServerProtect to Control Manager,

Initiating Automatic Update on Control Manager

After you have registered ServerProtect to Control Manager, you must configure settings on the Control Manager server to initiate automatic component update on the ServerProtect computer.

To initiate automatic update from Control Manager:

1. Make sure you have successfully registered ServerProtect to Control Manager.

2. Log on to the Control Manager Web console and select **Product Programs** in the **Manual Download** or **Scheduled Download** screen.

3. From Control Manager, perform a component update.

Refer to *Introducing Trend Micro Control Manager*™ on page A-1 or the Trend Micro Control Manager Administrator's Guide for more information about managing products in Control Manager.

World Virus Tracking Program

Trend Micro's World Virus Tracking Program (WVTP) collects Internet threat data from a vast number of corporate and individual computer systems around the world.

To participate in this program, click **Administrator > World Virus Tracking** and select the **Yes** option. Then click **Save** to make the changes take effect.

Configuring and Performing Scans with ServerProtect

This chapter discusses the following topics:

Types of Scanning

During installation, the ServerProtect setup program automatically detects the version of Linux being used on the server and installs the appropriate Kernel Hook Module (KHM). This means that ServerProtect on your Linux server is able to perform real-time scanning in addition to manual and scheduled scans.

If the setup program does not support the Linux version detected, KHM does not install. This means that ServerProtect can only perform manual and scheduled scans. It cannot perform real-time scanning. To install KHM on servers running Linux kernel versions ServerProtect does not support, you need to build (or compile) the KHM from the source code (refer to the appendix in the Getting Started Guide for detailed information).

The following describes the three types of scanning ServerProtect can perform:

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

- Scheduled scanning gives you an opportunity to do a periodic check on 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. Since 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.

- Manual scanning allows you to perform 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.

Note: To find out more about the scanning technologies ServerProtect employs, refer to *The ServerProtect for Linux Solution* on page 1-3.

The following sections shows you how to configure each scan type.

Configuring Real-Time Scan

When enabled, real-time scanning runs in the background, constantly checking all accessed files. Trend Micro recommends that you keep the Real-time Scanning option enabled at all times.

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

- **Incoming files**—Scan files that are being closed on the ServerProtect computer.
- **Outgoing files**—Scan files that are being opened on the ServerProtect computer.
- **Running applications**—Scan files that are being executed on the ServerProtect computer. For example, when you start an application.

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. Select the **Incoming files**, **Outgoing files**, and/or **Running applications** check boxes, to activate the desired scan target.
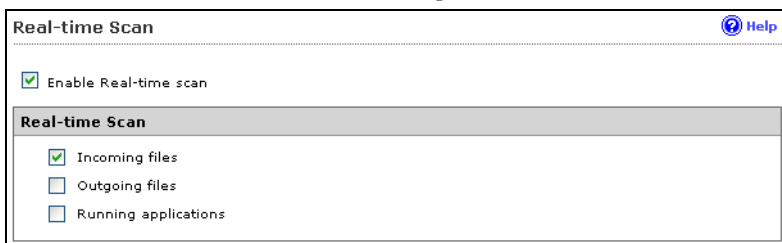
FIGURE 3-1.   Activating and configure real-time scan

4. Click **Save** to apply the setting.

Note: Trend Micro recommends keeping real-time scanning enabled. Real-time Scan is enabled by default.
To configure other scanning settings, refer to *Configuring Scan Settings* on page 3-8.

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

To configure 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.

FIGURE 3-2. Activating and configure scheduled scan

To configure scan frequency for a scheduled scan:

1. Click **Scan Options** > **Scheduled Scan** on the left menu.

2. To configure 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.

3. Click **Save** to apply the settings. To configure other scanning settings, refer to *Configuring Scan Settings* on page 3-8.

Invoking Scheduled Scan from the Command Line

From the command line, you can type `./splxmain` (in the `/opt/TrendMicro/SProtectLinux/SPLxvsapiapp` folder) to run a scheduled scan immediately. ServerProtect applies the scheduled scan settings saved in `tmsplx.xml`.

To invoke scheduled scan:

Type the following 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 in the `/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp` folder:

  ```
  ./splxmain -t
  ```

- From the task bar in X Window, click **Start Applications Menu** > **System (Tools)** > **Trend Micro ServerProtect** > **Stop Scheduled Scan**.

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 configure other scanning settings, refer to *Configuring Scan Settings* on page 3-8.

Note: ServerProtect cannot run a scheduled scan and a manual scan at the same time. If you try to start a manual scan while a scheduled scan is already in progress, a warning message screen displays. Wait until the scheduled scan is complete or stop it (using the `./splxmain -t` command) before you start a manual scan.

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

- In the Web browser, click `Scan now` from the **Summary** screen.
- From the task bar in X Window, click **Start Applications Menu** > **System (Tools)** > **Trend Micro ServerProtect** > **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 *Exclusion List* on page 3-14.
3. Click **Save & Scan**. The following confirmation window displays.
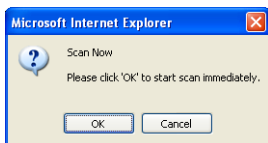
FIGURE 3-3.   Scan Now confirmation window

4. Click **OK** to begin the scan. The scan progress window appears showing the status of the scan.
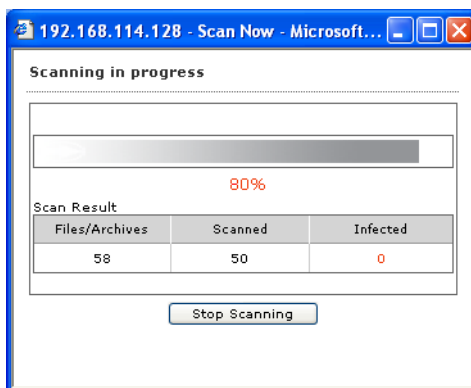
FIGURE 3-4. Scan progress window

Note: The time for a manual scan to complete varies depending on the file size and the number of files to scan. Trend Micro recommends that you perform a manual scan during off-peak hours or that you close other applications before you start a manual scan.

To run manual scan through the command line:

Run the following command in the
`/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp` folder:

```
./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
```

To stop a manual scan:

• Click **Stop Scanning** in the scan progress window.

• Run the following command:

```
./splxmain -n
```

• From the task bar in X Window, click **Start Applications Menu** > **System (Tools)** > **Trend Micro ServerProtect** > **Manual Scan > Stop Scan Now**.

Configuring Scan Settings

You configure each scan options in separate Web screens. However, they share several common components:

- Directories to scan
- Types of files to scan
- How to handle compressed files
- Actions on infected files
- Directories or files to exclude

The following sections describe each components in detail.

Configuring Scanning Directories

To specify locations to scan:

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

FIGURE 3-5. Select directories to scan

The options are:

- **All directories**—scans all directories, except those included in the Exclusion List. For additional information, refer to *Exclusion List* on page 3-14.

- **Specified directories only**—limits the scan to the directories and subdirectories that you specify. To do so:

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

    Note: The directory path names are case-sensitive.

    ii. Click **Add** to add the entry to the **Specified directories only** list.

    iii. Add other directories as required.

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

Note: For Real-time Scan, Manual Scan and Scheduled Scan, you can use the asterisk (*) or question mark (?) wildcards for the scan directories.

To remove directories that you previously specified:

1. Select the directory for removal in the **Scan these directories** list.

2. Click **Remove** 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 **Scan These Files**, specify the desired file types to scan.
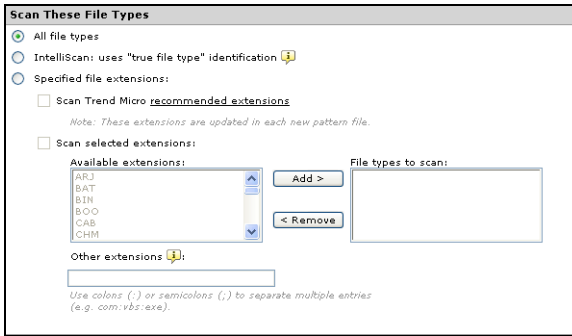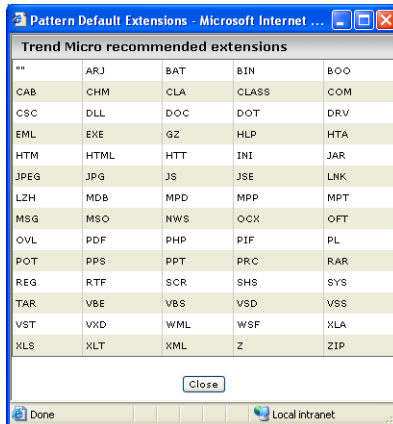
FIGURE 3-6.   Selecting file types to scan

The options are:

- **All file types**—Scans all files, except for those specified in the Exclusion List screen (refer to *Exclusion List* on page 3-14).

- **IntelliScan: uses "true file type" identification**—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.

- **Specified file extensions**—Restricts scanning to selected file extensions. This option 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:

FIGURE 3-7. 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 **Add >** 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 **< Remove** to remove the extension.

3. Click **Save** to apply your settings.
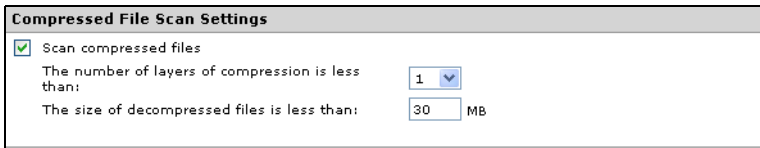
Scanning Compressed Files

Since compressed file scanning is a resource-intensive process, it is important to configure ServerProtect so it can efficiently 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 Scan Settings** section, select the **Scan compressed files** check box.

FIGURE 3-8.   Compressed file scanning

3. Specify the number of compression layers (1-20) to scan. 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 system log.

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

Specifying Actions on Infected Files

You can perform a variety of actions on detected viruses, as shown in the table below.

TABLE 3-1.   Actions that ServerProtect can take against detected viruses

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.

To specify actions on infected files:

1. On the left menu, select **Scan Options**, then choose the scan method.

2. Under the **Actions When Security Risks Found** section, select the **Back up file containing security risk before action is taken** check box to create a backup copy of the file before ServerProtect attempts to clean it. Trend Micro recommends selecting this option for the rare occasions when malware may damage a file in a way that does not allow cleaning, and as a result, the affected file is not recoverable.

3. Select the scan action. The options are described below.

    •   **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), specify the first action for each type of security risk (joke, Trojan, virus, test virus, spyware/grayware, and others). For virus, packer and other threats, select a second action. For example, for a virus, you might want to select **Clean** as the first action, and **Quarantine** as the second action.

    Note: If ServerProtect is unable to perform both the first and second actions on the detected file, the log entry is still counted once in the uncleanable category.

- **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, packer and other threats, and only when **Clean** is selected as the first action.

Action When Security Risk Found

☑ Back up file containing security risk before action is taken. 🛈

Select an action to take when detecting a security risk:

○ Use ActiveAction - recommended actions by file type 🛈
○ Use customized action

Type	First Action	Second Action
Joke	Quarantine	
Trojan	Quarantine	
Virus	Clean	Quarantine
Test Virus	Pass	
Spyware/Grayware	Quarantine	
Packer	Clean	Quarantine
Other	Clean	Quarantine

◉ Use the same action for all types

Type	First Action	Second Action
All Types	Clean	Quarantine

FIGURE 3-9. **Specify scan actions**

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.

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.

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

The following describes the type of lists you can configure to be excluded from scanning:

- **Directories to exclude**—Use this list to exclude whole directories from scanning.

- **Files to exclude**—Use this list to exclude specified files from scanning.

- **File types to exclude**—This list prevents ServerProtect from scanning specific file types.

WARNING! Real-time Scan will not function if the list of directories to exclude is empty.

Using Wildcard Characters

For Manual Scan and Scheduled Scan, 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: For Real-time Scan, ServerProtect does not support wildcards in the exclusion list or the list of extensions to scan. Doing so may cause unexpected scan results.

FIGURE 3-10. Exclusion list

Specifying the Quarantine Directory

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 the Quarantine Directory:

1. Select **Scan Options** > **Quarantine Directory** on the left menu. The Quarantine Directory screen displays.

2. Specify the full path of the 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 in the Backup Directory screen. The default backup 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 for each scan type.**

To specify the 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.

Chapter 4

Update

ServerProtect ships with scan engine and pattern files that are current at the time of the product release. The most recent threats may not be addressed by these components, Trend Micro recommends that you update them immediately after installing ServerProtect.

Topics discussed in this chapter include the following:

About ActiveUpdate

ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of pattern files and the scan engine for ServerProtect.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. Updates are available on a regularly scheduled interval that you configure, or on-demand.

Component Updates

In ServerProtect, the following components or files are updated through ActiveUpdate, the Trend Micro Internet-based component update feature:

•   *Virus/Spyware/Grayware Pattern*—These files contain 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 regularly 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. See the Getting Started Guide for more information on product registration and activation.

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

Specifying a Download Source

Depending on whether or not ServerProtect is being managed by Control Manager, the download source differs.

- When ServerProtect is being managed by 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 Control Manager updates is:

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

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

- When ServerProtect is not being managed by Control Manager, you can update components only using the Update Now (Manual Update) function. The default download source is:

`http://splx3-p.activeupdate.trendmicro.com/activeupdate`

To customize the download source:

1. Configure manual (see *Manual Update* starting on page 4-6) or scheduled update (see *Scheduled Updates* starting on page 4-7).

2. Select one of the following download sources:

   - **Trend Micro ActiveUpdate 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.

Configuring Proxy Server Settings

If you use a proxy server to access the Internet, you can configure proxy settings for the following features in ServerProtect:

- World Virus Tracking
- License update
- Component update

To configure proxy settings for World Virus Tracking and License update:

1. Click **Administration > Proxy Settings**. The General screen displays:
2. Select the **Use a proxy server to access the Internet** check box.
3. Select **HTTP**, **SOCKS4** or **SOCKS5** in the **Proxy Protocol** field.
4. In the **Server name or IP address** field, type the IP address or host name of the proxy server.
5. In the **Port** field, type the proxy server listening port number.
6. If you are using an optional proxy authentication user name and password, type this information in the **User name** and **Password** fields.
7. Click **Save**.

FIGURE 4-1.   Proxy Settings General screen
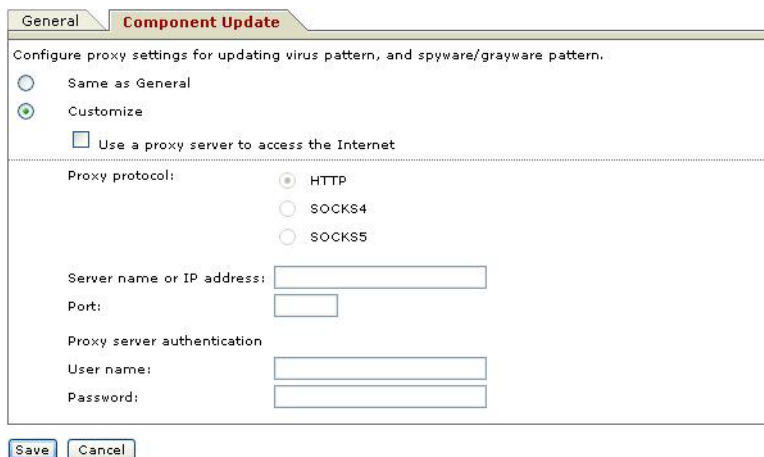
> **Tip:** Trend Micro recommends updating the virus pattern file and scan engine immediately after installation. If you use a proxy server to access the Internet, configure your proxy server settings before updating the scan engine and pattern file.

To configure proxy settings for component updates:

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

FIGURE 4-2.   Proxy Settings Component Update screen

2. Select **Same as General** to use the same proxy server setting you configure in the General screen.

3. Select **Customize** to configure the proxy settings.

4. Select **Use proxy server to access the Internet** if you want to use a proxy server for component update. Then continue to Step 5.

    Clear the **Use proxy server to access the Internet** check box if you do not want to use a proxy server for component updates. For example if the update server is located within your company network. Then skip to Step 9.

5. Select **HTTP, SOCKS4** or **SOCKS5** in the **Proxy Protocol** field.

6. In the **Server Name or IP Address** field, type the IP address or host name of the proxy server.

7. In the **Port** field, type the proxy server listening port number.

8. If you are using an optional proxy authentication user name and password, type this information in the **User name** and **Password** fields.

9. Click **Save**.

> **Note:** To set the proxy password from the command prompt, refer to *Using splxmain* on page B-37.

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 several ways to perform a manual update:

- Click **Update Now** from the Summary or Manual Scan screen.
- From the task bar on the main KDE window, click **Start Applications Menu > System (Tools) > Trend Micro ServerProtect > Start Update Now**.

To perform a manual update from the Summary screen:

1. Select **Summary** in the left menu.

2. In the **Component Status** section, select the **Component** check box to update all components or select check boxes to update individual components.

3. Click **Update Now**.

To perform a manual update from the Manual Update screen:

1. Select **Update > Manual Update** on the left menu. The Manual Update screen appears.

2. Select the check box of the component you want to update. The current version of each component appears to the right of the component label. Select the **Component** check box to select all components.

3. Next, specify a download source. Refer to *Specifying a Download Source* on page 4-2 for more information.

FIGURE 4-3. Manual Update screen

4. Click **Save** to save the settings. Click **Update Now** to save the settings and perform a manual scan.

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.

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 component you want to update. The current version of each component appears to the right of the component label. Select the **Component** check box to select all components.

4. Select a download source.

    You can set up multiple backup update servers/sources for automatic 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.

    ---

5. Select a start time in hours and minutes from the **Start time** menu.

6. 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.

    ---

7. Configure a download schedule. Refer to *Specifying a Download Source* on page 4-2 for more information.

FIGURE 4-4.   Scheduled Update screen

8. Click **Save**.

Chapter 5

Logs

This chapter discusses the following topics:

- *Types of Logs* on page 5-2
- *Viewing Scan Results (Logs)* on page 5-3
- *Configuring Notifications* on page 5-9

Types of Logs

ServerProtect offers four types of logs:

- **Spyware Log**—The spyware log reports spyware/grayware detections, including detection date and time, threat name, scan type, action taken and result, and the location of the source file in which the spyware/grayware was found.

- **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.

- **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.

- **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.

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 logs screens in the Web console

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.
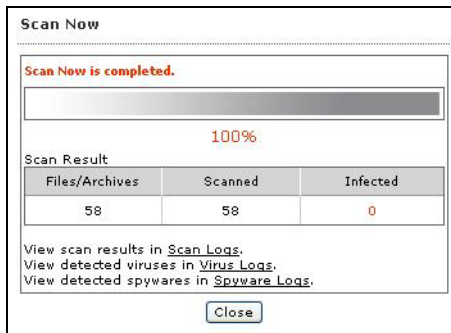
FIGURE 5-1.   Scan Now complete window

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.

Using the Log Screens in the Web Console

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:

- **Data Range**—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 **Data Range** 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 **Data Range** to use this criteria. The month-day-year format is used. Alternatively, click the calendar icon (▦) and select a date from the calendar.

- **Sort by**—Specify the order and grouping of the logs. Options for groups are: **Date/Time**, **Virus Name**, **Scan Type**, **Action Result**, and **Source Files**; the order may either be ascending or descending.

- **Entries 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.
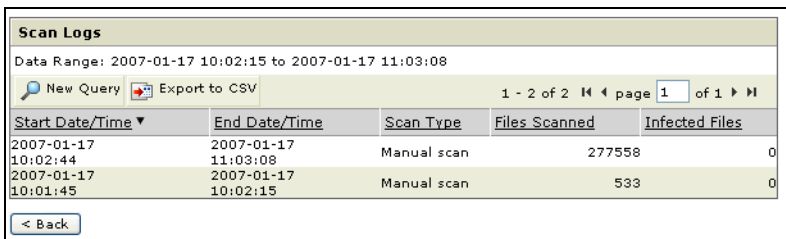
Note: You can increase the number of "logs to be queried" in the configuration file. See *MaxRetrieveCount* on page B-29 for more information.

---

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

   See the following figure for an example of the scan log:

FIGURE 5-2.   Scan log example

See the following figure for an example of the virus log:

Virus Detections

Data Range: 2007-01-10 11:57:36 to 2007-01-10 11:57:36

New Query   Export to CSV   1 - 1 of 1 ◄ page 1 of 1 ►

Date/Time ▼	Virus Name	Scan Type	Action Result	Source File
2007-01-10 11:57:36	HTML_IFRMEXP.GEN	Scheduled scan	Clean failed Quarantined	/usr/lib/mailman/tests/msgs/nimda.txt

< Back

FIGURE 5-3.   Virus log example

See the following figure for an example of the system log.

System Logs

Data Range: 2007-01-17 00:34:03 to 2007-01-17 07:17:48

New Query   Export to CSV   1 - 9 of 9 ◄ page 1 of 1 ►

Date/Time ▼	Description	Reason
2007-01-17 07:17:48	Real-time scan has been enabled.	
2007-01-17 07:11:55	Real-time scan has been disabled.	
2007-01-17 05:56:02	Real-time scan has been enabled.	
2007-01-17 05:50:03	Real-time scan has been disabled.	
2007-01-17 01:04:10	ActiveUpdate Fail	Unable to connect to the update server. Please verify the network connection is enabled and functional, and then try again. (http://splx3-p.activeupdate.trendmicro.com/activeupdate)
2007-01-17 01:00:02	License Reminder	The ServerProtect license grace period expires in 13 days
2007-01-17 00:54:08	ActiveUpdate Fail	Unable to connect to the update server. Please verify the network connection is enabled and functional, and then try again. (http://splx3-p.activeupdate.trendmicro.com/activeupdate)
2007-01-17 00:44:05	ActiveUpdate Fail	Unable to connect to the update server. Please verify the network connection is enabled and functional, and then try again. (http://splx3-p.activeupdate.trendmicro.com/activeupdate)
2007-01-17 00:34:03	ActiveUpdate Fail	Unable to connect to the update server. Please verify the network connection is enabled and functional, and then try again. (http://splx3-p.activeupdate.trendmicro.com/activeupdate)

< Back

FIGURE 5-4.   System log example

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 (◄ page 1 of 10 ►). To refresh the data, use the refresh function of the web

browser for this frame. 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, refresh this screen. Any activity that occurred between the previous query and the refresh are added to the log results.

Specifying the Log Directory Location

Scan, spyware, 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 in the Web console:

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

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

Deleting Logs
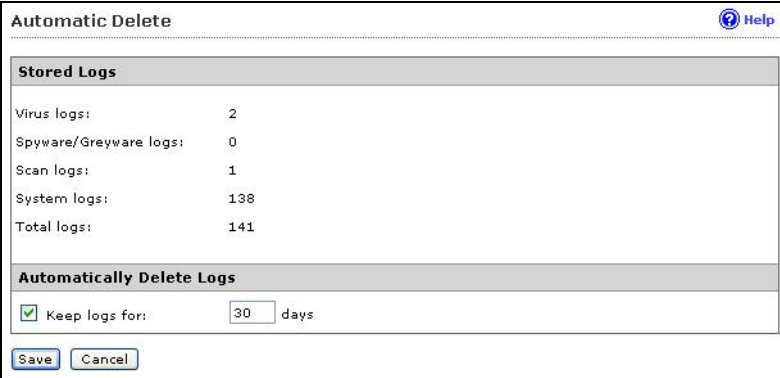
You can configure ServerProtect to delete logs automatically or manually. You can specify to delete all logs or delete logs that are older than the specified time.

Automatically Deleting Logs

To prevent logs from accumulating and consuming disk space, ServerProtect limits the time period of which logs are stored. By default, ServerProtect stores logs for 60 days after which they are automatically deleted.

To configure automatic log deletion in the Web console:

1. Click **Logs > Automatic Delete**.

2. To disable automatic log deletion, clear the **Keep logs for** check box. Select this check box to enable the feature and type the number of days to store logs in the field provided.

3. Click **Save** to save the changes.

FIGURE 5-5.   Automatic Delete

4. A screen displays indicating the number of days ServerProtect keeps logs. Click **OK** to return to the previous screen.

FIGURE 5-6.   Automatic Delete Settings Saved

Manually Deleting Logs

At any time, you can manually delete logs that were created before the specified date. This prevents logs from accumulating and consuming disk space.

To manually delete logs in the Web console:

1. Click **Logs > Manual Delete**.

2. To manually delete all logs, select **All Logs**. To delete logs that were created before the specified date, select **Logs before this date** and click the calendar icon (▦) to select a date.

3. Click **Delete** to save the changes.
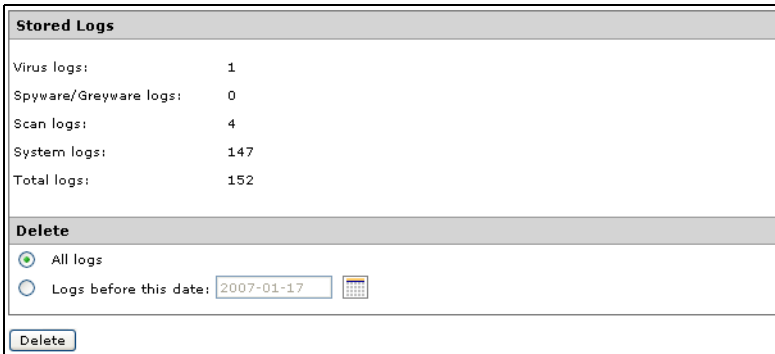
FIGURE 5-7. Manual Delete

4. A screen displays prompting you to confirm. Click **OK** to delete the logs.

FIGURE 5-8. Manual Delete Confirmation

5. A screen displays showing the result of the manual delete action. Click **OK** to return to the previous screen.

Manual Delete

Log deletion completed.
141 log(s) deleted.

Stored Logs

Virus logs:	0
Spyware/Greyware logs:	0
Scan logs:	2
System logs:	9
Total Logs:	11

OK
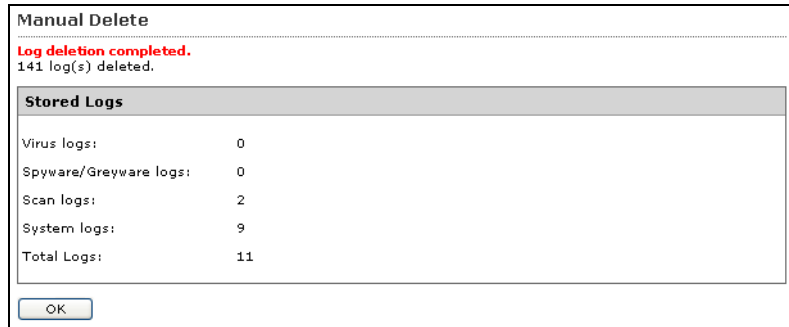
FIGURE 5-9.   Manual Delete Result

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 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.

- **Notification when pattern file update unsuccessful—**This alert triggers a notification if the pattern file update is not successful.

- **Notification when action performed on malware unsuccessful—**This alert triggers a notification if ServerProtect is unable to perform specified action(s) on the detected malware.

3. Each alert event provides a default notification message. See the following figure for an example.

FIGURE **5-10.** Notification Alert 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. You can specify up to 1024 printable ASCII characters.

Note: A notification message will not accept the "\n" characters.

---

2. Click **Save** when you are finished.

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

FIGURE 5-11. Notification Recipients

To enable SMTP mail notification:

1. Select **Notification** > **Recipients** from the left menu.
2. Select the **Enable 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 the mail account information in the **User Name** and **Password** fields.

6. Type your email address in the **From** field.

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

7. Click **Save**.

To add a recipient address:

1. Click **Notification > Recipients** from the left menu.

2. Type the recipient's full email address in the **Enter email address** field, for example:

    ```
    yourname@yourCompany.com
    ```

3. Click **Add >** to add the entry to the **Alert Recipients** list.

4. Click **Save**.

To remove a recipient address:

1. Select an address from the **Alert Recipients** list.

2. Click **< Remove** to remove the selected entry from the recipients list.

3. 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 6

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 does not have a default password. Trend Micro recommends setting a password 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 the splxhttpd status. For additional information, see *Using splxhttpd* on page B-43.
- **Java plug-in not installed properly—**This may happen if you are using the Mozilla, Mozilla Firefox or Internet Explorer browsers. Contact technical support if you need assistance.

Automatic Component Update

Configure automatic updates from Control Manager after successfully registering ServerProtect to Control Manager. For more information, see *Initiating Automatic Update on Control Manager* on page 2-18.

System Logs Related to ServerProtect

The following ServerProtect system logs may be created on your Linux machine. These logs will not affect the performance or operation of ServerProtect or your Linux computer.

```
splx_vsapiapp: [MODULE_NAME - CXIpc::connectToServer2] errno=2
```

```
some error were found while stopping entity. Force terminating
it
```

Debug Logging

ServerProtect 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

Configuring syslog-ng for SUSE Linux

To allow ServerProtect to store debug log information on SUSE Linux Enterprise Desktop/Server 10, you need to configure settings for syslog-ng (next generation).

1. Open the `syslog-ng.conf` file located in `/etc/syslog-ng/` and add the following lines into the file.

   ```
   # this is for splx debug log
   filter f_splx                        { facility(local3); };
   # logs for splx debug
   destination splx_debug_log { file("/var/log/splx.debug"); };
   log {source(src); filter(f_splx);
   destination(splx_debug_log); };
   ```

2. Restart the syslog daemon by typing `/etc/init.d/syslog restart` in the terminal.
3. Set the debug key (`UserDebugLevel`) in the `tmsplx.xml` file to 5.
4. Restart ServerProtect by typing `service splx restart`.

After you have configured the settings, ServerProtect stores debug information to the `splx.debug` file in `/var/log/`. You can open this file to see the debug logs.

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 6-1.   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 disabling it immediately after issue replication. Is is also recommended that your logs be on a non-root partition.

Enabling Debug Logging

Modify `tmsplx.xml` and `syslog.conf` to enable ServerProtect debug logging.

To enable debug logging:

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

WARNING! Making incorrect changes to a configuration file can cause serious system errors. Back up tmsplx.xml and syslog.conf to restore your original settings. After modifying the syslog.conf file, restart the syslog service immediately before you continue.

---

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

   b. To assign the path and filename where ServerProtect will write debug logs, edit `/etc/syslog.conf` on RHEL4 or RHEL5 platforms. For SLES10 or SLED10, please refer to *Configuring syslog-ng for SUSE Linux* on page 6-3 for more information.

   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.

   `ps -ef | grep syslogd` (RHEL4 or RHEL5)

   `ps -ef | grep syslog-ng` (SLES10 or SLED10)

4. Reload configuration.

   `kill -HUP <syslogd PID>` (RHEL4 or RHEL5)

   `kill -HUP <syslog-ng PID>` (SLES10 or SLED10)

> **Note:** To prevent Linux file operation errors, restart syslog before you restart the ServerProtect service.

5. Restart ServerProtect service:

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

Disable Debug Logging

Modify `tmsplx.xml` and `syslog.conf` to disable ServerProtect debug logging.

To disable debug logging:

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

> **WARNING!** 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**, then type save, and close `tmsplx.xml`.

3. Delete or comment out the debug path and filename in the following file depending on your platform.

   `/etc/syslog.conf` (RHEL4 or RHEL5)

   `/etc/syslog-ng` (SLES10 or SLED10)

4. Restart ServerProtect service:

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

> **Note:** To prevent Linux file operation errors, restart the ServerProtect service before you restart syslog.

5. Query PID.

```
ps -ef | grep syslogd (RHEL4 or RHEL5)
```

```
ps -ef | grep syslog-ng (SLES10 or SLED10)
```

6. Reload configuration.

```
kill -HUP <syslogd PID> (RHEL4 or RHEL5)

kill -HUP <syslog-ng PID> (SLES10 or SLED10)

etc/init.d/splx restart
```

Using logrotate

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 logrotate man page for details on logrotate.

To use logrotate:

1. Using a text editor such as vi, open `/etc/logrotate.d/syslog`.

WARNING! Making incorrect changes to a configuration file can cause serious system errors. Before you start, back up tmsplx.xml in case you need to restore your original settings.

---

2. Add the following lines to rotate logs:

```
/var/log/messages /{path}/{splxlog} {

    sharedscripts

    postrotate

    /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2>
    /dev/null || true

    endscript

}
```

3. Save and close the `syslog` file.

6-7

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:

`http://subwiz.trendmicro.com/SubWiz/Default.asp`

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[SM] 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 do not (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 through 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.

About Trend Micro

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway–gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of risks to information, by offering centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point, before they ever reach the desktop.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

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

Appendix A

Introducing Trend Micro Control Manager™

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services, third-party antivirus and content security products at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up-to-date. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

This chapter discusses the following topics:

Control Manager Basic Features

Control Manager is designed to manage antivirus and content security products and services deployed across an organization's local and wide area networks.

FEATURE	DESCRIPTION
Centralized configuration	Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console This helps ensure consistent enforcement of your organization's virus and content security policies.
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus outbreak
Secure communication infrastructure	Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
Secure configuration and component download	These features allow you to configure secure management console access and component download
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager management console users. User accounts define what the user can see and do on a Control Manager network. Track account usage via user logs.
Command Tracking	This feature allows you to monitor all commands executed using the Control Manager management console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.
On-demand product control	Control ServerProtect for Linux in real-time. Control Manager immediately sends configuration modifications made on the management console to the ServerProtect for Linux. System administrators can run manual scans from the management console. This command system is indispensable during a virus outbreak.
Centralized update control	Update virus patterns, anti-spam rules, scan engines, and other antivirus or content security components to help ensure that all managed

TABLE A-1.   Control Manager Features

FEATURE	DESCRIPTION
Centralized reporting	Get an overview of the antivirus and content security product performance using comprehensive logs and reports. Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

TABLE A-1.   Control Manager Features

Understanding Trend Micro Management Communication Protocol

Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP replaces TMI as the way Control Manager communicates with ServerProtect for Linux. MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- Two-way communication support
- Single sign-on (SSO) support
- Cluster node support

Reduced Network Loading and Package Size

TMI uses an application protocol based on XML. Even though XML provides a degree of extensibility and flexibility in the protocol design, the drawbacks of applying XML as the data format standard for the communication protocol consist of the following:

- XML parsing requires more system resources compared to the other data formats such as CGI name-value pair and binary structure (the program leaves a large footprint on your server or device).
- The agent footprint required to transfer information is much larger in XML compared with other data formats.
- Data processing performance is slower due to the larger data footprint.

- Packet transmissions take longer and the transmission rate is less than other data formats.

MCP's data format is devised to resolve the issues mentioned above. MCP's data format is a BLOB (binary) stream with each item composed of name ID, type, length and value. This BLOB format has the following advantages:

- **Smaller data transfer size compared to XML:** Each data type requires only a limited number of bytes to store the information. These data types are integer, unsigned integer, Boolean, and floating point.

- **Faster parsing speed:** With a fixed binary format, each data item can be easily parsed one by one. Compared to XML, the performance is several times faster.

- **Improved design flexibility:** Design flexibility is also been considered since each item is composed of name ID, type, length and value. There will be no strict item order and compliment items can be present in the communication protocol only if needed.

In addition to applying binary stream format for data transmission, more than one type of data can be packed in a connection, with/or without compression. With this type of data transfer strategy, network bandwidth can be preserved and improved scalability is also created.

NAT and Firewall Traversal Support

With limited addressable IPs on the IPv4 network, NAT (Network Address Translation) devices have become widely used to allow more end-point computers to connect to the Internet. NAT devices achieve this by forming a private virtual network to the computers attached to the NAT device. Each computer that connects to the NAT device will have one dedicated private virtual IP address. The NAT device will translate this private IP address into a real world IP address before sending a request to the Internet. This introduces some problems since each connecting computer uses a virtual IP and many network applications are not aware of this behavior. This usually results in unexpected program malfunctions and network connectivity issues.

For products that work with TMCM 2.5/3.0 agents, one pre-condition is assumed. The server relies on the fact that the agent can be reached by initiating a connection from server to the agent. This is a so-called two-way communication product, since both sides can initiate network connection with each other. This assumption breaks when agent sits behinds a NAT device (or TMCM server sits behind a NAT device) since the

connection can only route to the NAT device, not the product behind the NAT device (or the TMCM server sitting behind a NAT device). One common work-around is that a specific mapping relationship is established on the NAT device to direct it to automatically route the in-bound request to the respective agent. However, this solution needs user involvement and it does not work well when large-scale product deployment is needed.

Manual Configuration for Communication via NAT

To work around Control Manager communication in a NAT network, either using the one-way or two-way communication model, you need to configure settings in the `Agent.ini` and `Product.ini` files and set up port forwarding.

Step 1: Set the public IP address in the Agent.ini file

Open the `Agent.ini` file in the `/opt/TrendMicro/SProtectLinux` folder and type the public IP address of the NAT device for the `IPAddressList` parameter.

Step 2: Set the TMCM protocol name in the Product.ini file

Open the Product.ini file in the `/opt/TrendMicro/SProtectLinux` folder and type "http" or "https" for the `ProtocolName` field.

Note: If you type "https", you must also set the `port` parameter to "14943".

Step 3: Configure port forwarding rules on the NAT device

You must set port forwarding rules on the NAT device to forward traffic to the ServerProtect server behind the NAT device on port 14942 (HTTP) or 14943 (HTTPS). Port forwarding rule:

Public IP (port: 14942/14943) => Private IP (port: 14942/14943)

HTTPS Support

The MCP integration protocol applies the industry standard communication protocol (HTTP/HTTPS). HTTP/HTTPS has several advantages over TMI:

• A large majority of people in IT are familiar with HTTP/HTTPS, which makes it easier to identify communication issues and find solutions those issues

- For most enterprise environments, there is no need to open extra ports in the firewall to allow packets to pass
- Existing security mechanisms built for HTTP/HTTPS, such as SSL/TLS and HTTP digest authentication, can be used.

Using MCP, Control Manager has three security levels:

- **Normal security:** Control Manager uses HTTP for communication
- **Medium security:** Control Manager uses HTTPS for communication if HTTPS is supported and HTTP if HTTPS is not supported
- **High security:** Control Manager uses HTTPS for communication

Two-Way Communication Support

MCP supports two-way communication.

Two-Way Communication

Two-way communication is an alternative to one-way communication. It is still based on one-way communication, but has an extra channel to receive server notifications. This extra channel is also based on HTTP protocol. Two-way communication can improve real time dispatching and processing of commands from the server by the Control Manager agent. The Control Manager agent side needs a Web server or CGI compatible program that can process CGI-like requests to receive notifications from Control Manager server.

Single Sign-on (SSO) Support

Through MCP, Control Manager 3.5 now supports single sign-on (SSO) functionality for Trend Micro products. This feature allows users to sign in to Control Manager and access the resources of other Trend Micro products without having to sign in to those products as well.

The following products support SSO with Control Manager 3.5:

- ServerProtect for Linux version 3.0
- Network VirusWall Enforcer 1200
- Network VirusWall Enforcer 2500

Cluster Node Support

Under varying cases administrators may like to group certain product instances as a logical unit, or cluster (for example products installed under a cluster environment present all installed product instances under one cluster group). However, from the Control Manager server's perspective, each product instance that goes through the formal registration process is regarded as an independent managed unit and each managed unit is no different from another.

Through MCP, Control Manager supports cluster nodes.

Control Manager Agent Heartbeat

To monitor the status of ServerProtect for Linux, Control Manager agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the ServerProtect for Linux and to check for commands to the ServerProtect for Linux from Control Manager. The Control Manager Web console then presents the product status. This means that the ServerProtect for Linux status is not a real-time, moment-by-moment reflection of the network's status. Control Manager checks the status of each ServerProtect for Linux computer in a sequential manner in the background. Control Manager changes the status of ServerProtect for Linux to offline, when a fixed period of time elapses without a heartbeat from the ServerProtect for Linux computer.

Active heartbeats are not the only means Control Manager has for determining the status of the ServerProtect for Linux computer. The following also provide Control Manager with the ServerProtect for Linux status:

- Control Manager receives logs from the ServerProtect for Linux. Once Control Manager receives any type of log from the ServerProtect for Linux successfully, this implies that the ServerProtect for Linux is working fine.

- In two-way communication mode, Control Manager actively sends out a notification message to trigger the ServerProtect for Linux to retrieve the pending command. If server connects to the ServerProtect for Linux successfully, it also indicates that the product is working fine and this event will be counted as a heartbeat.

-

The Control Manager agent heartbeats implement with the following ways:

- **UDP:** If the product can reach the server using UDP, this is the most lightweight, fastest solution available. However, this does not work in NAT or firewall environments. Also the transmitting client cannot make sure that the server does indeed receive the request.

- **HTTP/HTTPS:** To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the ServerProtect for Linux computer applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains ServerProtect for Linux computer activity information to display on the console.

Using the Schedule Bar

Use the schedule bar in the Communicator Scheduler screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

Blue slots denote Working status or the hours that the Communicator sends information to the Control Manager server. White slots indicate Idle time. Define Working or Idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity.

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest Communicator status information and the need to manage system resources. Trend Micro's default settings is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval Heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status on the Control Manager management console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).
Short-interval Heartbeats (below 60 minutes)	Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.

TABLE A-2.   Heartbeat Recommendations

Registering ServerProtect to Control Manager

ServerProtect for Linux is a standalone product and you do not need to register the computer on which it is installed to Control Manager. However, by registering to Control Manager you gain the benefits explained earlier in this appendix. All features are managed using the ServerProtect for Linux Web console. Before registering a ServerProtect for Linux computer to a Control Manager server, you must ensure that both the ServerProtect for Linux computer and the Control Manager server belong to the same network segment.

You can register the ServerProtect for Linux computer to Control Manager during the installation process or using the Web console.

To check status on Control Manager:

1. From the Control Manager management console **Main Menu**, click **Products**.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.

3. Check to see that the ServerProtect for Linux computer displays.

Managing ServerProtect for Linux Computers From Control Manager

A managed product refers to a computer on which ServerProtect for Linux is installed, an antivirus, a content security or third party product represented in the Product Directory. The Control Manager management console represents managed products as icons. These icons represent the ServerProtect for Linux computers, other Trend Micro antivirus and content security products, as well as third party products.

Indirectly administer the managed products either individually or by groups through the Product Directory. Use the Directory Manager to customize the Product Directory organization.
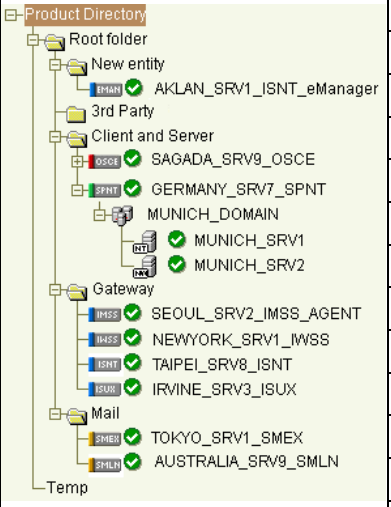
Understanding Product Directory

Take care when planning the structure of the Product Directory, a logical grouping of managed products, because it affects the following:

- **User access:** When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. Carefully plan the Product Directory since you can only grant access to a single segment. For example, granting access to the root segment grants access to the entire Directory. On the other hand, granting access to a specific ServerProtect for Linux computer only grants access to that specific product.

- **Deployment planning:** Control Manager deploys virus pattern, scan engine, spam rule, and program updates to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory will therefore simplify the designation of recipients.

- **Outbreak Prevention Policy and Damage Control Template deployments:** OPP and DCS deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

As shown in this sample Product Directory, managed products identify the registered antivirus or content security product, as well as provide the connection status.

A-11

Product Directory icons:

PRODUCT DIRECTORY TREE	ICON	DESCRIPTION
Product Directory Root folder New entity AKLAN_SRV1_ISNT_eManager 3rd Party Client and Server SAGADA_SRV9_OSCE GERMANY_SRV7_SPNT MUNICH_DOMAIN MUNICH_SRV1 MUNICH_SRV2 Gateway SEOUL_SRV2_IMSS_AGENT NEWYORK_SRV1_IWSS TAIPEI_SRV8_ISNT IRVINE_SRV3_ISUX Mail TOKYO_SRV1_SMEX AUSTRALIA_SRV9_SMLN Temp		New entity or user-defined folder name
	EMAN	InterScan eManager
	OSCE	OfficeScan Corporate Edition
	SPNT	ServerProtect Information Server
		ServerProtect Domain
	NT	ServerProtect for Windows (Normal Server)
	NW	ServerProtect for NetWare (Normal Server)
	IMSS	InterScan Messaging Security Suite
	IWSS	InterScan Web Security Suite
	ISNT	InterScan VirusWall for Windows
	ISUX	InterScan VirusWall for UNIX
	SMEX	ScanMail for Microsoft Exchange
	SMLN	ScanMail for Lotus Notes
	NVW	
	NVW.	Network VirusWall
	NVW	
	FW	NetScreen Global PRO Firewall
	✓	Managed Product connection status icon

TABLE A-3. Managed Product Icons

Arrange the Product Directory using the Directory Manager. Use descriptive folders to group your ServerProtect for Linux computers according to their protection type and the Control Manager network administration model. For example, grant access rights to mail administrators to configure the Mail folder.

Accessing a ServerProtect for Linux Default Folder

Newly registered ServerProtect for Linux computers usually appear in the New entity folder depending on the user account specified during the agent installation. Control Manager determines the default folder for the ServerProtect for Linux computer by the privileges of the user account specified during the product agent installation. However, Control Manager segregates managed products handled by Trend VCS agents under the Trend VCS agents folder.

The following presents different scenarios for the accessible folders given to the account and the resulting default managed product location:

ACCESSIBLE FOLDER GIVEN TO THE ACCOUNT	DEFAULT MANAGED PRODUCT LOCATION
Root folder	New entity
Mail	Mail
SAGADA_SRV9_OSCE	New entity

User accounts set to access a specific managed product cannot access any newly registered managed products.

TABLE A-4.   Managed Products vs. User Access

Access Product Directory

Use the Product Directory to administer ServerProtect for Linux computers registered with the Control Manager server.

Note: Viewing and accessing the folders in the Product Directory depends on the Account Type and folder access rights used to log on to the management console.

To access the Product Directory:

1. Click **Products** on the main menu.

2. On the left most menu, select **Managed Products** from the list and then click **Go**.

Manually Deploy New Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your ServerProtect for Linux computer and other managed products on demand. This is useful especially during virus outbreaks.

Download new components before deploying updates to specific or groups of ServerProtect for Linux computers or managed products.

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu.

2. On the left most menu, select **Managed Products** from the list and then click **Go**.

3. On the left-hand menu, select the desired folder or ServerProtect for Linux.

4. On the working area, click the **Tasks** tab.

5. Select **Deploy <component>** from the Select task list.

6. Click **Next>>**.

7. Click **Deploy Now** to start the manual deployment of new components.

8. Monitor the progress via Command Tracking.

9. Click the **Command Details** link to view details for the Deploy Now task.

View ServerProtect for Linux Status Summaries

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all ServerProtect for Linux and other managed products present in the Product Directory tree.

There are two ways to view the ServerProtect for Linux status summary:

- Through Home page
- Through Product Directory

To access through the Home page

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through Product Directory:

1. Click **Products** on the main menu.
2. On the left-hand menu, select the desired folder or ServerProtect for Linux.
   - If you click a ServerProtect for Linux computer or managed product, the Product Status tab displays the ServerProtect for Linux computer or managed product's summary
   - If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries

---

Note: By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last month available in the Display summary for list.

Configure ServerProtect for Linux and Managed Products

Depending on the product and agent version:

- You can configure devices or products either individually or in groups according to folder division

  Perform group configuration using the folder Configuration tab.

> **Note:** When performing a group configuration, verify that you want all ServerProtect for Linux computers in a group to have the same configuration. Otherwise, add devices or managed products that should have the same configuration to Temp to prevent the settings of other managed products from being overwritten.

- The Configuration tab shows either the product's Web console or a Control Manager-generated console

To configure a product:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired ServerProtect for Linux computer, managed product or folder.
4. On the working area, click the **Configuration** tab.

> **Note:** Step 4 is necessary when you use the folder Configuration tab.

---

5. Select the product to configure from the Select product list.
6. At the Select configuration list, select the product feature to access or configure.
7. Click **Next**. The ServerProtect for Linux or managed product Web-based console or Control Manager-generated console appears.

Issue Tasks to ServerProtect for Linux and Managed Products

Use the Tasks tab to invoke available actions to a group or specific ServerProtect for Linux computer or managed product. You can perform the following tasks on a ServerProtect for Linux computer:

- Configuration Replication
- Deploy engines
- Deploy pattern files/cleanup templates
- Enable/disable real-time scan
- Start/stop manual scan (Scan Now)

- Command Tracking of all commands

Deploy the latest pattern file, or scan engine to ServerProtect for Linux with outdated components. To successfully do so, the Control Manager server must have the latest components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to ServerProtect for Linux:

1. Access the Product Directory.
2. On the left-hand menu, select the desired ServerProtect for Linux or folder.
3. On the working area, click the **Tasks** tab.
4. Select the task from the Select task list.
5. Click **Next**.
6. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Query and View ServerProtect for Linux Computer and Managed Product Logs

Use the Logs tab to query and view logs for a group or specific ServerProtect for Linux computer.

To query and view ServerProtect for Linux logs:

1. Access the Product Directory.
2. On the left-hand menu, select the desired ServerProtect for Linux or folder.
3. On the working area, click the **Logs** tab.
4. Select the client log type:

   Event Logs:

   a. Provide the following search parameters:

PARAMETER	DESCRIPTION
Severity	Refers to the degree of information available. The options are: Critical, Warning, Information, Error, Unknown. Select the check box of your chosen parameter

TABLE A-5.   Search Parameters for Event Logs

PARAMETER	DESCRIPTION
Incident	Refers to events. The options are: All events, Virus outbreak, Module update, Service On, Service Off, Security violation, Unusual network virus behavior
Product	If you select a folder, this list shows the managed products belonging to the folder. To view information on all products, select All. Otherwise, query logs of a specific managed product
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE A-5. Search Parameters for Event Logs

b. Click **Display Logs** to begin the query and display the query results.

Security Logs:

a. Select All virus log incidents or a specific security logs type and then click **Query**.

b. Provide the following search parameters:

PARAMETER	DESCRIPTION
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE A-6. Search Parameters for Security Logs

    c. Click **Display Logs** to begin the query.

Note: eManager managed products records content security violations in the Security Logs, not in the Virus Logs.

---

5. The Query Result screen displays the results in a table format.

6. The Generated at entity column of the result table indicates the Control Manager server time.

Recover ServerProtect for Linux Computer Removed From the Product Directory

The following scenarios can cause Control Manager to delete a ServerProtect for Linux computer from the Product Directory:

• Reinstalling the Control Manager server and selecting Delete existing records and create a new database option

    This option creates a new database using the name of the existing one.

• Replacing the corrupted Control Manager database with another database of the same name

• Accidentally deleting the ServerProtect for Linux computer using the Directory Manager

If a Control Manager server's ServerProtect for Linux computer records are lost, the agents on the products still "know" where they are registered to. The product agent will automatically re-register itself after 8 hours or when the service is restarts.

To recover ServerProtect for Linux computer removed from the Product Directory, restart the ServerProtect for Linux computer.

Search for ServerProtect for Linux Computers, Product Directory Folders or Other Computers

Use the Search button to quickly:

• Add a specific or a group of ServerProtect for Linux computers to Temp

• Find and locate a specific ServerProtect for Linux computer in the Product Directory

To search for a folder or ServerProtect for Linux computer:

1. Access Product Directory.

2. On the left menu, click **Search**.

3. On the working area, provide the following search parameters:

PARAMETER	DESCRIPTION
Search for	Select the object of the search from the drop down list Search for managed products or Communicators based on their name, folder name, or computer name.
Keyword	This allows you to search for the object by name Select **Case sensitive** to narrow down the search results.
Managed product status / Communicator status	Select the appropriate connection status, for the Communicator or managed product The options are: All, Active, Inactive, Abnormal, Product Active, and Product Inactive. Choose All to search for objects regardless of the connection status.
Product	Select the appropriate product from the list. Choose **All** to search for all products.

TABLE A-7.   Search Parameters

4. Click **Begin Search** to start searching.

5. Control Manager presents the search results in a table format. You may opt to directly create the temp sub-folder where the search results will be grouped.

Refresh the Product Directory

To refresh the Product Directory:

•   In the Product Directory, click the **Refresh** icon on the upper right corner of the left menu.

Understanding Directory Manager

After the registering to Control Manager, the ServerProtect for Linux first appears in the Product Directory under the default folder.

Use the Directory Manager to customize the Product Directory organization to suit your administration model needs. For example, you can group products by location or product-type   messaging security, web security, file storage protection, and so on.

The Directory allows you to create, modify, or delete folders, and move ServerProtect for Linux computers between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the ServerProtect for Linux computers belonging to each folder. Consider the following factors when planning and implementing your folder and ServerProtect for Linux computer structure:

• Product Directory

• User Accounts

• Deployment Plans

Group ServerProtect for Linux computers according to geographical, administrative, or product specific reasons. In combination with different access rights used to access ServerProtect for Linux computers or folders in the directory, the following table presents the recommended grouping types as well as their advantages and disadvantages:

Grouping Type	Pro's	Con's
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

TABLE A-8.   Product Grouping Comparison

Using the Directory Manager Options

Directory Manager provides seven options: New Folder, Delete, Rename, Undo, Redo, Cut, and Paste.

Use these options to manipulate and organize ServerProtect for Linux in your Control Manager network.

To use and apply changes in the Directory Manager:

- Right-click a folder or ServerProtect for Linux computer to open a pop-up menu that presents a list of actions you can perform
- Click **+** or the folder to display the ServerProtect for Linux computers belonging to a folder
- Press **Enter** or click anywhere when you rename a folder
- Click **Save** to apply your changes and update the Directory Manager organization
- Click **Reset** to discard changes that are not yet saved

Access Directory Manager

Use Directory Manager to group ServerProtect for Linux computers together.

To access the Directory Manager:

1. Access Product Directory.
2. On the left-hand menu, click **Directory Manager**.

Create Folders

Group ServerProtect for Linux computers into different folders to suit your organization's Control Manager network administration model.

To create a folder:

1. Access the Directory Manager.
2. On the working area, right-click where you want to create a new folder. If you are building the tree for the first time, right-click the Root folder.
3. Select **New folder** from the pop-up menu. Control Manager creates a new sub-folder under the main folder.
4. Type a name for the new folder or use the default name and then press **Enter**.
5. Click **Save**.

Except for the New entity folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, _, {, |, }, and ~), numbers (0 to 9), or alphabet characters (a/A to z/Z).

Renaming Folders or ServerProtect for Linux

To rename a folder or ServerProtect for Linux:

1. Access Directory Manager.
2. On the working area, right-click the folder or ServerProtect for Linux computer you want to rename and then select **Rename** from the pop-up menu. The folder/ServerProtect for Linux name becomes an editable field.
3. Type a name for the new folder or use the default name and then press **Enter**.
4. Click **Save**.

Note: Renaming a ServerProtect for Linux computer only changes the name stored in the Control Manager database. There are no effects to the product.

Move Folders or ServerProtect for Linux Computer

To transfer or move a folder or ServerProtect for Linux to another location:

1. Access Directory Manager.
2. On the working area, select the folder or ServerProtect for Linux computer you want to move.
3. Do one of the following:
    *   Drag-and-drop the folder or ServerProtect for Linux to the target new location
    *   Cut and paste the folder or ServerProtect for Linux to the target new location
4. Click **Save**.

Delete User-Defined Folders

Take caution when deleting user-defined folders in the Directory Manager, you may accidentally delete a ServerProtect for Linux computer which causes it to unregister from the Control Manager server.

To delete a user-defined folder:

1. Access the Directory Manager.
2. On the working area, right-click the folder you want to delete and then select **Delete** from the pop-up menu.
3. Click **Save**.

Note: You cannot delete the New entity folder.
Use caution when deleting user-defined folders, you may accidentally delete a
ServerProtect for Linux computer.

Understanding Temp

Temp, a collection of ServerProtect for Linux shortcuts, allows you to focus your attention on specific products without changing the Product Directory organization. Use Temp for deploying updates to groups of products with outdated components.

Consider the following issues when using Temp:

- Control Manager deletes all ServerProtect for Linux shortcuts when you log off the management console.
- You can only add the ServerProtect for Linux to Temp if you can see them in the Product Directory, you cannot make shortcuts to products that you cannot access.

Using Temp

You can manipulate ServerProtect for Linux computers in Temp the same way you would with ServerProtect for Linux computers in the Product Directory. The folders and ServerProtect for Linux computers belonging to Temp have the same folder and ServerProtect for Linux-level controls. However, Control Manager determines what actions you can perform on the ServerProtect for Linux according to your user account's access rights.

You can use Temp for the following purposes:

- Issue commands to groups of ServerProtect for Linux computers using folder-level access rights.
- Select a specific ServerProtect for Linux computer, and then use the available Product Directory tabs to perform an action.

Access Temp

Use Temp to collect ServerProtect for Linux shortcuts.

To access Temp:

1. Access Product Directory.
2. On the left most menu, click **Temp**.

Adding ServerProtect for Linux computers to Temp

There are three methods to add ServerProtect for Linux computers to Temp:

- From the Search results
- From the Product Directory
- Add ServerProtect for Linux computers with outdated components based on the Status Summary page

Trend Micro recommends that you add several ServerProtect for Linux computers at once to Temp using the last method. The Status Summary screen provides information as to which ServerProtect for Linux computers use outdated components. It simplifies virus pattern and scan engine updates on groups of ServerProtect for Linux computers belonging to different folder groups.

Note: Adding ServerProtect for Linux computers to Temp only allows you to collect ServerProtect for Linux computers with outdated components doing so does not trigger automatic deployment.

To add from the Search results

1. Click **Products** on the main menu.
2. On the left-hand menu, click **Search**.
3. On the working area, search for ServerProtect for Linux computers or folders.

4. Specify a sub-folder name in the **Temp sub-folder for managed products** field for the Temp sub-folder that will contain the ServerProtect for Linux shortcuts.

Note: Step 4 is optional. If you want to create multiple folder levels belonging to Temp, specify \{folder name level1}\{sub-folder name level2} in the Temp sub-folder for entities field. For example, if you specify \pattern\mail, the following Temp structure appears:

---

5. Click **Add**. Control Manager adds the ServerProtect for Linux computers from the search results to Temp.

To add from the Product Directory

1. Access the Product Directory.
2. On the left-hand menu, select the ServerProtect for Linux computer you want to add to Temp.
3. Press "+" on the numeric keypad.

To add a ServerProtect for Linux computer with outdated components based on the Status Summary page:

1. Access Product Directory.
2. On the left-hand menu, select the desired Product Directory folder.
3. On the working area, click the **Product Status** tab.
4. At the Component Status table, click one of the numeric links indicating the number of ServerProtect for Linux computers that are outdated. Depending on the link you clicked, the Virus Pattern Status (Outdated), Scan Engine Status (Outdated), Spam Rule Status (Outdated) screen opens displaying the computer name, product name, product version, and outdated component version.

5. Click **Add to Temp** in the status page. Control Manager organizes the ServerProtect for Linux computers to Temp using folders named after the page from which they were added. For example, Control Manager places ServerProtect for Linux computers added from the Scan Engine Status (Outdated) page under the Scan Engine Status (Outdated) folder.

> **Note:** Clicking **Add to Temp** only adds the ServerProtect for Linux computers shown on the status page. If the list of ServerProtect for Linux computers spans more than one screen, click **Add to Temp** on all screens to add all products with outdated component.

6. Click **Back** to return to the Status Summary page, and then proceed to the next outdated component. Repeat the instructions until Control Manager adds all the outdated ServerProtect for Linux computers to Temp.

Removing a ServerProtect for Linux Computer From Temp

To remove a ServerProtect for Linux computer from Temp:

1. Access Product Directory.
2. On the left-hand menu, click **Temp**.
3. From the available ServerProtect for Linux computer on the Temp list, select the folder or ServerProtect for Linux shortcut that you want to remove.
4. Press "-" in the numeric keypad.

> **Note:** Control Manager removes ServerProtect for Linux shortcuts in Temp when you log off from the management console.
>
> Removing a ServerProtect for Linux computer from Temp will neither disconnect the antivirus or content security product nor uninstall the Control Manager agent from the Control Manager server.

Download and Deploy New Components From Control Manager

Update Manager is a collection of functions that help you update the antivirus and content security components on your Control Manager network. Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats. By default, Control Manager enables virus pattern, damage cleanup template, and Vulnerability Assessment pattern download even if there is no managed product registered on the Control Manager server.

The following are the components to update (listed according to the frequency of recommended update):

• **Pattern files**—refer to virus and spyware/grayware scan pattern files, Pattern Release History, and network virus and spyware/grayware pattern files

Note: Only registered users are eligible for components update. For more information, see the Control Manager online help Registering and Activating your Software > Understanding product activation topic.

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed product.

Understanding Update Manager

Update Manager provides functions that help you update the antivirus and content security components of your Control Manager network.

Updating the Control Manager network involves two steps:

• Downloading components: You can do this manually or by schedule
• Deploying components: You do this manually or by schedule

Understanding Manual Downloads

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Manually Download Components

This is the Trend Micro recommend method of configuring manual downloads. Manually downloading components requires multiple steps:

Tip: Ignore steps 1 and 2 if you have already configured your deployment plan and configured your proxy settings.

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download settings

Step 5: Configure the automatic deployment settings

Step 6: Complete the manual download

To manually download components:

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.

3. On the working area, click **Add New Plan**.

4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.

5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.

6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:

- **Delay**—After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

  Use the menus to indicate the duration, in terms of hours and minutes.

- **Start at**—Performs the deployment at a specific time

  Use the menus to designate the time in hours and minutes.

7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

8. Click **OK**.

9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

1. Click **Administration > System Settings**. The System Settings screen appears.

System Settings

Control Manager can use a variety of access and communication methods. Provide the required data to take advantage of these options.

Save

ActiveUpdate settings
☐ Enable HTTPS for the default update download source
Local Windows Authentication
User name: guest
Password: ******
Remote UNC Authentication
User name: guest
Password: ******

Download component proxy settings
☐ Use a proxy server to download update components from the Internet
Host name: [　　　] Port: 80
For example, proxy.company.com or 10.21.254.30
Protocol: ⦿ HTTP ○ Socks
Authentication
Login name: [　　　]
Password: [　　　]

Trend VCS agent proxy settings
☐ Use a proxy server to connect to Trend VCS agents
Host name: [　　　] Port: 80
For example, proxy.company.com or 10.21.254.30
Protocol: ⦿ HTTP ○ Socks
Authentication
Login name: [　　　]
Password: [　　　]

Notification settings
SMTP server
Host name: [　　　] Port: [　　]
For example, proxy.company.com or 10.21.254.30
Sender email address: rice_tseng@trend.com.tw
Note: The SMTP server may need a sender address to deliver mail.
Pager COM port
Use [　▼] for pagers
SNMP trap notification
Community name: [　　　]
Server IP address: [　　　]
Trigger application
☐ Use an specified user to trigger application
User name: guest
Password: ******
MSN(TM) Messenger notification
MSN(TM) Messenger email address: [　　　]
Password: [　　　]
☐ Use a proxy server to connect to MSN(TM) server
Host name: [　　　] Port: 1080
For example, proxy.company.com or 10.21.254.30
Protocol: ⦿ Socks 4 ○ Socks 5
Authentication:
Login name: [　　　]
Password: [　　　]

Save

2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.

3. Type the host name or IP address of the server in the **Host name** field.

4. Type a port number in the **Port** field.

5. Select the protocol:

   • **HTTP**

   • **SOCKS**

6. Type a logon name and password if your server requires authentication.

7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration > Update Manager > Manual Download**. The Manual Download screen appears.

2. From the Components area select the components to download.

    a. Click the + icon to expand the component list for each component group.

    b. Select the components to download.

Step 4: Configure the download settings

1. Select the update source:

    •   **Internet: Trend Micro update server:** Download components from the official Trend Micro ActiveUpdate server.

- **Other update source:** Type the URL of the update source in the accompanying field.

  After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.

2. Select Retry frequency and specify the number or retries and duration between retries for downloading components.

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 5: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:

   - **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually
     - Testing the updated components before deployment
   - **Deploy immediately:** Components download to Control Manager, then deploy to managed products
   - **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select
   - **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.

3. Click **Save**.

Step 6: Complete the manual download

1. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.

2. Click the **Command Details** to view details from the Command Details screen.

3. Click **OK** to return to the Manual Download screen.

Configure Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire day(s) or for a certain time every day.

This feature particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

To configure scheduled download exceptions:

1. Click **Administration** on the main menu.

2. On the left-hand menu under Update Manager, click **Scheduled Download Exceptions**.

3. Do the following:

   • To schedule a daily exception, under Daily schedule exceptions, select the check box of the day(s) to prevent downloads, and then select the **Do not download updates on the specified day(s)** check box. Every week, all downloads for the selected day(s) are blocked.

   • To schedule an hourly exception, under Hourly schedule exceptions, select the hour(s) to prevent downloads, and then select the **Do not download updates on the specified hour(s)** check box. Every day, all downloads for the selected hours are blocked.

4. Click **Save**.

Understanding Scheduled Downloads

Configure scheduled downloading of components to keep your components up-to-date and your network secure. Control Manager supports granular component downloading. You can specify the component group and individual component download schedules. All schedules are autonomous of each other. Scheduling downloads for a component group, downloads all components in the group.

Use the Scheduled Download screen to obtain the following information for components currently in your Control Manager system:

- **Frequency:** Shows how often the component is updated
- **Enabled:** Indicates if the schedule for the component is either enabled or disabled
- **Update Source:** Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download schedule

Step 5: Configure the download settings

Step 6: Configure the automatic deployment settings

Step 7: Enable the schedule and save settings

Configure Scheduled Downloads and Enable Scheduled Component Downloads

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.

3. On the working area, click **Add New Plan**.

4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.

5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.

6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:

   • **Delay**—After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

   Use the menus to indicate the duration, in terms of hours and minutes.

- **Start at**—Performs the deployment at a specific time

    Use the menus to designate the time in hours and minutes.

7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

8. Click **OK**.

9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

1. Click **Administration > System Settings**. The System Settings screen appears.

2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.

3. Type the host name or IP address of the server in the **Host name** field.

4. Type a port number in the **Port** field.

5. Select the protocol:

    - HTTP
    - SOCKS

6. Type a logon name and password if your server requires authentication.

7.   Click **Save**.

Step 3: Select the components to update

1.   Click **Administration > Update Manager > Scheduled Download**. The
     Scheduled Download screen appears.

2.   From the Components area select the components to download.

   a.   Click the + icon to expand the component list for each component group.

   b.   Select the components to download:

        The <Component Name> screen appears. Where <Component Name> is the
        name of the component you selected.

Pattern files/Cleanup templates

Schedule automatic component download below.

☐ **Enable scheduled download**

Schedule and frequency

Download: ○ Every [5 minutes ▼]

○ Every [hour ▼]

◉ Every [day ▼]

○ Every [week ▼] on [Sunday ▼]

Start time: [00 ▼] : [53 ▼] (hh:mm)

Download settings

Source: ◉ Internet: Trend Micro update server

○ Other update source

[http://   ] [+] [-]

for example, http://DownloadServer.Antivirus.com/AU or
c:\ActiveUpdate\ or \\updatesource

Retry frequency: ☐ If the download is unsuccessful, retry [2] time(s), every [2] minute(s)

Proxy: (Edit)

Automatic deployment settings

Configure and select a Deployment Plan below to schedule automatic deployment by location.

Schedule: ○ Do not deploy

○ Deploy immediately

◉ Based on deployment plan

☑ When new updates found

Deployment plan: [Deploy to All Managed Products Now (Default) ▼]

[Save] [Cancel] [Reset]

Step 4: Configure the download schedule

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.

2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minute, hour, day, or week.

3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.

Step 5: Configure the download settings

1. Select the update source:

    • **Internet: Trend Micro update server:** Download components from the official Trend Micro ActiveUpdate server.

    • **Other update source:** Type the URL of the update source in the accompanying field.

      After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number or retries and duration between retries for downloading components.

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

---

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 6: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:

    • **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:

      • Deploying to the managed products individually

      • Testing the updated components before deployment

    • **Deploy immediately:** Components download to Control Manager, then deploy to managed products

    • **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select

    • **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

---

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

---

2. Select a deployment plan after components download to Control Manager, from the **Deployment plan** list.

3. Click **Save**.

Step 7: Enable the schedule and save settings

1. Click the status button in the Enabled column.

2. Click **Save**.

Use Reports

A Control Manager **report** is an online collection of figures about virus, spyware/grayware, and content security events that occur on the Control Manager network. The Enterprise edition provides the Control Manager reports.

Control Manager 3.5 categorizes reports according to the following types:

- Local reports
- *Global reports*

> **Note:** You can only configure the **Global Report Profile** option through the *parent server management console.*

Local Reports

Local reports are reports about managed products administered by the parent server. Local reports do not include reports generated by child servers. Use the Global Report options to view reports about managed products administered by child servers registered to the parent server.

Use Local Reports screen to view available one-time-only and scheduled local report profiles.

To access Local Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Local Report Profile**.

> **Note:** When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Global Reports

Global reports are reports about managed products administered by child servers as well as the parent server.

Use Global Reports screen to view available one-time-only and scheduled global report profiles.

To access Global Reports:

1. Click **Reports** on the main menu.

2. On the left most menu under Reports, click **Global Report Profile**.

3. When multiple reports are available, sort reports according to Report Profile or Last Created date.

Note: Only the parent server can display the global report profiles.

When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Understanding Report Templates

A report template outlines the look and feel of Control Manager reports. In particular, a template defines which sections appear in a report:

- Headers
- Report body
- Footers

Trend Micro Control Manager 3.5 adds 3 new report templates to the 77 previously available since Service Pack 3. The reports added in Service Pack 3 fall into five categories: Desktop, Fileserver, Gateway, Mailserver and Executive Summary. The new reports in Control Manager 3.5 fall into a new 6th category: Network Products. This category offers reports related to Network VirusWall.

Note: In Control Manager 3.5 spyware/grayware are no longer considered viruses. This change effects the virus count in all original virus related reports.

To generate these reports, click **Reports** on the main menu, then click **Create Report Profile** under Local Report Profile on the navigation menu. In the Contents tab that appears in the working area, you can type a report name, an optional report title and an optional report description. Use the **Report Category** list to peruse the six categories of reports listed below. Clicking a mark into a check box includes the associated report in the final exported report file.

Control Manager 3.5 also provides 18 templates stored in `<root>\Program Files\Trend Micro\Control Manager\Reports` as Crystal Report version 9 files (*.rpt). These templates also apply to Local and Global reports.

Understanding Report Profiles

A **profile** lays out the content (template and format), target, frequency, and recipient of a report. You can view reports in the following file formats:

- **RTF:** Rich text format; use a word processor (for example, Microsoft Word™) to view *.RTF reports
- **PDF:** Portable document format; use Adobe Reader to view *.PDF reports
- **ActiveX™:** ActiveX documents; use a Web browser to view reports in ActiveX format

Note: Control Manager cannot send reports in ActiveX format as email attachments.

- **RPT:** Crystal Report format; use Crystal Smart Viewer to view *.RPT reports

After generating the report, Report Server launches the default viewer for that report file format. For RPT reports, you must have the Crystal Smart Viewer installed.

Create Report Profiles

Creating a report profile is a five-step process. Creating local or global reports, the process stays very similar. The process to create a report profile is as follows:

Step 1: Select whether to create a local or global report

Step 2: Configure the Contents tab settings

Step 3: Configure the Targets tab settings

Step 4: Configure the Frequency tab settings

Step 5: Configure the Recipient tab settings

To create local or global report profile:

Step 1: Select whether to create a local or global report

1. Click **Reports** on the main menu.

2. Take one of the following actions:

   - To create a local report profile, click **Local Report Profile** under Reports.

   - To create a global report profile, click **Global Report Profile** under Reports.

3. On the left menu under Local Report Profile or Global Report Profile, click **Create Report Profile**.

Step 2: Configure the Contents tab settings

1. In the working area under the Contents tab, type a name for the report in the **Report name** field to identify the profile on the Local Reports screen.

2. Type a title for the report in the **Report Title** field (optional).

3. Type a description of the report profile in the **Description** field (optional).

4. Select **Network Products** from the **Select report template** list.

5. Select the report format.

6. Click **Next >** to proceed to the Targets tab.

Create Report Profile

| 1. Contents | **2. Targets** | 3. Frequency | 4. Recipients | 5. Summary |

Choose the managed product or managed product folder that will be the focus of the report.

Select multiple managed products or folders.

- Product Directory
  - ☐ Root folder
    - ☐ New entity

Selected Machines

- ◉ **All clients**
- ○ **IP range**
  - From :
  - To :
- ○ **Segment**
  - Example : 10.1.120.122 / 24 : means mask is : 255.255.255.000
  - Segment :   /

[< Back] [Next >] [Cancel]

Step 2: Configure the Contents tab settings

1. On the working area under the Targets tab, select the target of the local or global report profile:

   • Select the ServerProtect for Linux computer or folders. The profile only contains information about the ServerProtect for Linux computer or folders selected.

- Select the child servers. The profile only contains information about the child servers selected. Select the parent server to include all child servers' managed products in the profile.

2. Select the machines that the report will include:

   - **All clients:** All clients the selected ServerProtect for Linux protects
   - **IP range:** Select the IP range of the clients you want to include in the report
   - **Segment:** Select the IP range and segment of the clients you want to include in the report

3. Click **Next >** to proceed to the Frequency tab.

Create Report Profile

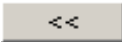| 1. Contents | 2. Targets | **3. Frequency** | 4. Recipients | 5. Summary |

Define when and how often this report is generated.

- ⦿ One-time only
  Contents in the report:
  From: February ▾ 22 ▾ 2006 ▾
  To: February ▾ 22 ▾ 2006 ▾

- ○ Daily

- ○ Weekly ▾ , on Sunday ▾

- ○ Every first day ▾ of the month

- ☐ Use calendar day

Start the scheduler:
- ⦿ Immediately
- ○ Start on
  February ▾ 22 ▾ 2006 ▾
  17 ▾ : 47 ▾ (hh:mm)

☑ Number of reports to keep 10 ▾

[< Back] [Next >] [Cancel]

Step 4: Configure the Frequency tab settings

1. On the working area under the Frequency tab, specify how often Control Manager generates this report. You have the following options:

   - **One-time only:** Provides information you specified in the From and To dates
   - **Daily:** Contains information from the creation time (12:00 AM yesterday) up to the current time

A-51

- **Weekly or Bi-weekly:** Contains 7 or 14 days worth of information; select the day of the week that will trigger the report server to generate a report
- **Monthly:** Contains 30 days worth of information; select the day of the month (first, 15th, or last day) that will trigger the report server to generate a report
- **Use calendar day:** If checked, the start time is 00:00:00 of the first day and the end time is 00:00:00 of the day before generation

  If it is not checked, the start time is the same generation hour of the first day and end time is the generation hour of the day when generation occurs

2. Under Start the scheduler, specify when the Report Server starts collecting information for this report. Select one of the following:
   - **Immediately:** The report server collects information as soon as you save the report profile
   - **Start at:** The report server collects information at the specified date and time
3. For scheduled reports, click **Number of reports to keep** and then specify the instance Control Manager will maintain on the server.

Note: Control Manager automatically enables a scheduled report profile. To temporarily disable generating reports, navigate to the Local or Global Scheduled Reports screen, and then clear the check box adjacent to the scheduled report profile.

---

4. Click **Next >** to proceed to the Recipient tab.

Create Report Profile

| 1. Contents | 2. Targets | 3. Frequency | **4. Recipients** | 5. Summary |

Send email notifications to the following recipients whenever Control Manager generates the report:

Users and groups
```
--- Group List ---
Unexpected_Event
Update_Event
Virus_Event

--- User List ---
root
```

Recipient list
```
--- Group List ---

--- User List ---
```

☑ Send the report as an attachment

[< Back] [Next >] [Cancel]

Step 5: Configure the Recipient tab settings

1. On the working area under the Recipients tab, select recipients from the existing Control Manager users and groups.

   - Use [>>] to add recipients from the **Users and groups** list to the Recipient list

   - Use [<<] to remove recipients from the **Recipient** list

2. Click **Send the report as an attachment** to send the report as an attachment. Otherwise, recipients will only receive an email notification about the report being generated.

3. Click **Next >** to proceed to the Summary tab.

Create Report Profile

| 1. Contents | 2. Targets | 3. Frequency | 4. Recipients | **5. Summary** |

Profile created at:	2/22/2006 5:48:35 PM
Created by:	root
Contents	
Report name:	SPLX Report Template 1
Report title:	
Report description:	
Export file format:	Rich Text Format
Report template:	1. Overall List of Spyware/Grayware Detected in All Entities
	2. Overall List of Viruses Detected in All Entities
	3. Overall Damage Cleanup Comparison
	4. Overall Spam Comparison
	5. Overall Spyware/Grayware Comparison
	6. Overall Virus Comparison
	7. Overall Most Commonly Detected Spyware/Grayware
	8. Overall Most Commonly Detected Viruses
	9. Overall Summary of Spyware/Grayware Detected
	10. Overall Viruses Detected

Targets

- Product Directory
  - ☑ Root folder
    - ☐ New entity
    - ☑ MCP Managed Products

4. On the working area under the Summary tab, review the profile settings and then click **Finish** to save the profile.

Review Report Profile Settings

Use the Profile Summary screen to review profile settings.

To access Profile Summary and review report profiles:

- Access Local or Global Reports

  On the working area under the Profile Summary column, click **View Profile**.

- Access Local or Global Scheduled Reports

  On the working area under the Profile Summary column, click **View Profile**.

Enable Scheduled Report Profiles

By default, Control Manager enables scheduled profiles upon creation. In an event that you disable a profile (for example, during database or agent migration), you can re-enable it via the Scheduled Local Reports or Scheduled Global Reports screen.

To enable scheduled report profiles:

1. Access Local or Global Scheduled Reports.

2. On the working area under Report Profiles column, click the profile check box.

   Click the check box adjacent to Report Profiles to select or deselect all profiles.

3. Click **Enable**.

Note: The options to enable, disable, and edit one-time-only profiles are not available because Control Manager generates these reports only once.

Generate On-demand Scheduled Reports

The Report Server generates scheduled reports based on the date and time you specified. When the date and time has not yet commenced, use **Run Now** to create scheduled reports on demand.

To generate on-demand scheduled reports:

1. Click **Reports** on the main menu.

2. Do one of the following:
   • To create a local report profile, click **Local Report Profile** on the left menu under Reports
   • To create a global report profile, click **Global Report Profile** on the left menu under Reports

3. On the working area under the Available Reports column, click the corresponding **View** link.

4. On the Available Reports for {profile name} under **Generate a {Frequency} report starting from**, specify the starting month, day, and year.

5. Click **Run Now**.

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the **View** link adjacent to the report becomes available.

View Generated Reports

Aside from sending and then viewing reports as email attachments, you can also use the Local Report Profile or Global Report Profile screen to view the available local or global reports.

To view reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
    *   To create a local report profile, click **Local Report Profile** on the left menu under Reports
    *   To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the Available Reports column, click the corresponding **View** link.

    On the Available Reports for {profile name}, you can sort reports according to **Submission Time** or **Stage Completion Time.**
4. Under the Status column, click **View Report**. The default program used to open the file format opens.

Appendix B

Configuration Commands

This appendix provides additional information about configuring ServerProtect using commands.

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
- `SProtectLinux.bin`: explains how to use the ServerProtect installer.
- `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

*   DESTINFO Group Key

*   SOURCEINFO Group Keys

> **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

*   WVTP 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.

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 SUSE Linux 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 priority over inclusion settings.

RealtimeScan

This key enables/disables Real-time Scan.

The valid values are:

    0 disable

    1 scan incoming (write) files (default)

    2 scan outgoing (read) 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 value to scan all directories.

RealtimeIntelliScan, ScheduledIntelliScan, ManualIntelliScan

Use this key to turn IntelliScan on or off from within the configuration file. The values are 0 = disable IntelliScan (default), 1 = enable IntelliScan.

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/mqueue:
/var/spool/mqueue.iscan:
/opt/TrendMicro/SProtectLinux/SPLX.Quarantine:
/opt/TrendMicro/SProtectLinux/SPLX.Backup:
```

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.

Type	First Action	Second Action
Joke	Quarantine	
Trojan	Quarantine	
Virus	Clean	Quarantine
Test Virus	Pass	
Spyware/Grayware	Quarantine	
Packer	Clean	Quarantine
Other	Clean	Quarantine

TABLE B-1. Default customized scan actions

For viruses, packer 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.

Type	First Action	Second Action
All Types	Clean	Quarantine

TABLE B-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`, `ManualCustomizedAction`, `RealtimeAllTypesAction`, `ScheduledAllTypesAction` and `ManualAllTypesAction` keys are set to zero, ServerProtect automatically uses ActiveAction for Real-time Scan, Scheduled Scan, and Manual Scan.

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

RealTimeScanArchived, ScheduledScanArchived, ManualScanArchived

This key is not used.

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 default value is "0". Valid 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, AlertServerProtectOff

These keys set ServerProtect to send an alert notification whenever the ServerProtect 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 sets ServerProtect to send an alert notification whenever the pattern file is out-of-date. The valid values are:

    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"/>
```

AlertPatternUpdateFail

This key controls whether ServerProtect sends an alert notification whenever the pattern file update is not successful.

    0 disable sending an alert notification whenever the pattern file update is not successful

    1 enable sending an alert notification whenever the pattern file update is not successful (default value)

AlertActionFail

This key controls whether ServerProtect sends an alert notification if ServerProtect is unable to perform specified action(s) on the detected malware.

    0 disable sending an alert notification whenever ServerProtect is unable to perform specified action(s) on the detect malware

    1 enable sending an alert notification whenever ServerProtect is unable to perform specified action(s) on the detect malware

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.

ScheduledMDay

This key sets the day of month a scheduled scan runs when the value of the `Schedule` key is `4` (once every month). The valid values are numbers 1 through 31, 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.

EngineType

This key should not be modified by users.

EngineVersion

This key should not be modified by users.

EngineLastUpdateTime
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.

PatternLastUpdateTime
This key should not be modified by users.

SpywarePatternType

This key should not be modified by users.

SpywarePatternVersion

This key should not be modified by users.

SpywarePatternDate

This key should not be modified by users.

SpywarePatternLastUpdateTime
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.

ManualNOption, ScheduledNOption

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

0   none

1   update virus pattern

2   update scan engine

3   update both virus pattern and scan engine

32   update spyware pattern

33   update virus pattern and spyware pattern

34   update spyware pattern and scan engine

35   update virus pattern, spyware pattern, and scan engine (default)

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`.

ScheduledWDay

This key sets the day of week for scheduled updates. The valid values are `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday` and `Sunday`.

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 when ServerProtect performs a scheduled update. 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 differs based upon whether or not ServerProtect is registered to Trend Micro Control Manager.

When ServerProtect is registered to Control Manager, 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 Control Manager, the default value is:

```
http://splx3-p.activeupdate.trendmicro.com/activeupdate
```

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

Source

This key contains an alternate source for downloading updates. The default value for this key is null. 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.

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

  1   enable digital signature download

Note: If you enable digital signature download (`DigSig = 1`) and that the download source is a Control Manager server, ActiveUpdate may fail as Control Manager does not provide digital signatures for download.

SrvAuth

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

- 0 disable digital signature download (default)

- 1 enable digital signature download

Merge

This key sets whether the ServerProtect allows incremental update to the pattern files when updating from ActiveUpdate. The valid values are:

- 0 disable

- 1 enable (default)

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 or the `splxmain` command (in the `/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp` folder. See *Using splxmain* on page B-37).

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

B-19

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.

ProxyType

Specify the proxy server type. The valid values are:

0   HTTP proxy (default)

1   socks4 proxy

2   socks5 proxy

UseGeneralProxy

This key instructs ServerProtect to download component updates from the update server using the same general proxy setting for WVTP and license update. The valid values are:

    0   do not use the general proxy server for component update (default)

    1   use the general proxy server for component update

`DESTINFO` Group Key

Destination

This key contains the default directory path for ServerProtect. 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`.

SmtpUserID

This key contains the user account name on the SMTP server. The default value is null.

SmtpPassword

This key contains the user account password on the SMTP server. The default value is null.

SmtpAuthType

This key is for internal usage. It records the method of authentication used to log on to the SMTP server, which is automatically detected by ServerProtect. The valid values are:

`0` do not need authentication (default)

`1` LOGIN method

`2` PLAIN method

3   CRAM_MD5 method

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 is not used in ServerProtect for Linux version 3.0.

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
```

PatternUpdateFailMessage

This key contains the subject line of the pattern update fail notification. The default value is:

```
[SPLX] Pattern update unsuccessful
```

ActionFailMessage

This key contains the subject line of the action fail notification. The default value is:

```
[SPLX] Action performed on malware unsuccessful
```

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.

ThreadNumber

This key should not be modified by users.

UserDebugLevel

Report level for debugging information from the user-level portion of ServerProtect. The valid values are:

0   No debug output

1   Only log function entry and the involved name/path (default)

2   Log more information than Level 1 about process ID, function return code, and more information about class members' function and data members' value

3   Log more information than Level 2 about internal data structures and additional information about the scan engine, virus pattern, and scanning data

4   Log more details than Level 3 about operation flows

5   Log all information

As a general rule, it is best to select level 5 to collect all debugging information when analyzing a problem.

KernelDebugLevel

Report level for debugging information from the kernel-level portion of ServerProtect. When this parameter is set to a non-zero value, additional messages about ServerProtect operations are logged to the system's syslog.conf(5) The valid values are:

0   No debug output (default)

1   Only log function entry and the involved name/path

2   Log more information than Level 1 about process ID, function return code, and more information about class members' function and data members' value

3   Log all information

As a general rule, it is best to select level 3 to collect all debugging information when analyzing a problem. This key only affects the information logged by the system logger into the file specified in the `syslog.conf` file (`/var/log/messages` by default). Refer to *Debug Logging* on page 6-3 to enable or disable debug logging.

ControlManagerDebug
The range is 0 to 3, with 0 meaning "disable." The default value is 1. For more information, see *Table 6-1* on page 6-4.

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.

Lang

This key should not be modified by users.

SessionTimeout

Web console session timeout value, in seconds. Default value is 1200 seconds (20 minutes).

`GUIPassword` **Group Keys**

user1

This key should not be modified by users.

BypassLocalLogin

This key sets ServerProtect to allow administrator logon without entering a password if you log on to the local machine. The default value is 0.

    0 do not bypass password checking for local logon

    1 bypass password checking for local logon

`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 typing the `./splxmain -g` in the command line (in the `/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp` folder). 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 this release, you can change the limit by specifying a number between 200 and 65535 for this parameter in the `tmsplx.xml` file. 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.
If the `MaxRetrieveCount` key value is set too small, the total number of virus/grayware logs in the **Summary** screen will be smaller than the actual count.

The Web console also allows you to choose how many log entries display per page. The valid values are 15, 25, 30, 50, 100, and 200.

`Registration` Group Keys

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

EnableScheduledOnlineUpdateLicense

This key indicates whether scheduled license update is activated on ServerProtect. The valid values are:

    0   disable scheduled license update

    1   enable scheduled license update (default)

ScheduledTime

This key sets the time (HH:MM:SS) for scheduled license update. The default time is 01:30:00.

PrServerRegisterURL

This key contains the URL for the product registration feature to obtain the Activation Code. This key should not be modified by users.

PrServerOnlineUpdateURL

This key contains the URL for online update. This key should not be modified by users.

PrServerRenewInstrURL

This key contains the URL for accessing the product license renewal instructions. This key should not be modified by users.

PrServerUpgradeInstrURL

This key contains the URL for accessing the product license upgrade instructions. This key should not be modified by users.

PrServerViewLicenseURL

This key contains the URL for accessing detailed product license information. This key should not be modified by users.

EnableProxy

This key indicates a proxy server is required to access the license update server. 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 EnableProxy key, set the proxy address, and if required, the username, password, and port number.

ProxyServer

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

proxy.company.com

ProxyType

This key sets the proxy server type.

0 HTTP proxy (default)

1 socks4 proxy

2 socks5 proxy

ProxyPort

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

ProxyUserID

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.

SessionTimeOut

This key sets the number of seconds to wait before terminating the connection to the Web server. Must be greater than 0. The default value is 10 seconds.

`WVTP` Group Keys

The keys in this group contain data used by ServerProtect for the World Virus Tracking Program (WVTP).

EnableWVTP

This key specifies whether the ServerProtect machine is to participate in WVTP:

    0 disable

    1 enable (default value)

CountryCode

This key should not be modified by users.

ServiceURL

This key should not be modified by users.

ScheduledTime

This key should not be modified by users.

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 (before the most recent update of `tmsplx.xml`).
`tmeplx.xml.template`—The configuration 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

The table below lists the general keys in the `RemoteInstall.conf` file, including whether they are configurable and their default values.

Key	Default value	Description
DeployOption	1	1 - ServerProtect package deployment and installation 2 - ServerProtect configuration file deployment 3 - KHM module deployment
Package Name	SProtectLinux-3.0.bin	Indicates the ServerProtect installation file path for package deployment
Activation Code/ SerialNumber	(empty)	The ServerProtect Activation Code 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.mod-ule/RHEL4/splx-mod-2.6.9-22.0.2.ELs mp.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*.
* Trend Micro recommends keeping this default value		

TABLE B-1. `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 the PID of syslogd (CentOS) or syslog-ng (SUSE) 3.Set syslogd or syslog-ng to reread its configuration: `(kill -HUP `PID`)`
StatusFile	splx_remote_status	Indicates the file name for deployment status.
FullStatus*	1	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 keeping this default value		

TABLE B-1. `RemoteInstall.conf` **keys, default values, and descriptions**

Note: Trend Micro recommends that you keep this default value.

Using `splxmain`

The `splxmain` command enables you to maintain and control ServerProtect from the command line. You can run this command in the `/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp` folder. 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 |-e |-f |-g <date> |-i |-j |-k |-l
<port> |-m <directory> |-n |-o |-q <Activation Code> |-r |-s
|-t |-u |-v |-w <port> |-W |-x |-y][-D |-E]
```

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.

B-37

-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.

-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 B-29.

-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.

-q <Activation Code> sets the Activation Code (also known as the 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. You can view the scheduled settings in the /etc/cron.d/splx file.

-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. Use this option only if you have disabled real-time scan with the -x option previously.

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

```
./splxmain -w 12345
```

B-39

-W Set the World Virus Tracking Program (WVTP) setting. Type yes or no to enable or disable this feature.

-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.

-D Force vsapiapp to run as a daemon. This option can be used with -e.

-E Query the current license status.

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`

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 Control Manager registration status.

Using `splxcore`

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`

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`

This tool is designed to avoid redundant scanning when installing Trend Micro InterScan VirusWall, InterScan Web Security Suite, InterScan Messaging Security Suite and ServerProtect on the same server.

The `splxcomp` script resides in the `/opt/TrendMicro/SProtectLinux/SPLX.util` folder.

Use `splxcomp` to locate and include the quarantine and backup directories for InterScan VirusWall, InterScan Web Security Suite or InterScan Messaging Security Suite to the Exclusion list.

Note: If you uninstall InterScan VirusWall, InterScan Web Security Suite or InterScan Messaging Security Suite from the ServerProtect computer, you must also remove the corresponding quarantine and backup directories from the Exclusion List. This prevents anyone from infecting the un-used directories with viruses/spyware.

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 `CMconfig`

You can use the CMconfig command to register ServerProtect to and unregister it from Trend Micro Control Manager (TMCM).

The CMconfig utility detects whether or not ServerProtect is registered to Control Manager. If ServerProtect is currently registered to Control Manager, CMconfig unregisters it. Otherwise, CMconfig prompts you to type the configuration information on the command line and registers ServerProtect to Control Manager.

Alternatively, you can save configuration settings in a file and use the -f option to specify the file name from which the CMConfig command is to get the information. The default template file tmcm_registration_template.ini contains all the configuration parameters.

Location:

    /opt/TrendMicro/SProtectLinux/SPLX.util

Syntax:

    CMconfig [-h] [-f] [-Q] [-P]

Parameters:

-f <input_file> gets configuration from an input file to register to
 Control Manager

-Q queries Control Manager agent status

-P specifies the Control Manager Web server authentication username/password

-h displays the tool's parameters list

Note: To specify a proxy type, change the Proxy_Type parameter in the Agent.ini
file (located in the /opt/TrendMicro/SProtectLinux/folder) before you use
the CMconfig command to register ServerProtect to Control Manager.

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/`

Index

X

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.

FIGURE 1-1.

Term	Explanation
activate	To enable your software after completion of the registration process. Trend Micro products will be installed as an evaluation version.Activate during installation or after installation (in the management console) in the Product License screen.
Activation Code	A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: 9U-HG53-857B-TD54-MMP8-7754-MPP0 *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 utility that you can run from the command line to register ServerProtect 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.

FIGURE 1-1.

Term	Explanation
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption.
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.
exploit	An exploit is code that allows a malicious hacker to take advantage of a software vulnerability or security hole.
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

FIGURE **1-1.**

Term	Explanation
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.
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.
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.

FIGURE 1-1.

Term	Explanation
IP	Internet Protocol—*See* IP address.
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 be removed from your system.
Konquerer Desktop Environment (KDE)	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 or above 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.

FIGURE 1-1.

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.

FIGURE 1-1.

Term	Explanation
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.
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.
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.
RemoteInstall	A ServerProtect utility that can be used 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 configuration on remote machines.
RemoteInstall.conf	The config file for the RemoteInstall utility
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.

FIGURE 1-1.

Term	Explanation
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.
Secure Sockets Layer (SSL)	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.

FIGURE 1-1.

Term	Explanation
Telnet	The Internet standard protocol for remote logon 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 logon 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.

FIGURE **1-1.**

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.
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.