Trend Micro™ ServerProtect™ 3.0

Administrator's Guide

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

SUSE Linux Enterprise Server 16

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

https://docs.trendmicro.com/en-us/enterprise/serverprotect.aspx

Trend Micro, the Trend Micro t-ball logo, ServerProtect, and Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2026. Trend Micro Incorporated. All rights reserved.

Document Part No.:

Release Date:

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

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

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 Notice:

https://www.trendmicro.com/privacy

Table of Contents

Preface

Preface 1

ServerProtect for Linux Documentation 2

Audience 2

Document Conventions 3

Chapter 1: Introduction

Main Features 1-2

- Managing ServerProtect Through Trend Micro Apex Central or Trend Micro Control Manager 1-2
- Reports Available from Apex Central / Control Manager .. 1-2
- Multiple-Processor Support 1-3
- Remote Management Through a Web Browser 1-3
- Manual, Real-Time, and Scheduled Scanning 1-3
- Application Execution Protection 1-3
- Backup Directory Configuration 1-3
- Detailed, Easy-to-Maintain and Exportable Logs 1-3
- Manual and Automated Log Deletion Options 1-4
- Manual or Automated Internet-Based Updates 1-4
- Notification of Virus Outbreaks 1-4
- Outbreak Prevention Services 1-4
- Award-Winning Software 1-5
- Command-Line Interface Support 1-5
- Support for Advanced ActiveUpdate Options 1-5
- Consistency Checking Between ServerProtect and Configuration File (tmsplx.xml) 1-6
- Support for Intel Hyper-Threading Technology 1-6
- Support for Trend Micro Online Registration System 1-6
- Options for Detailed Debugging 1-7
- Safer Configuration File Modifications 1-7
- IntelliScan and ActiveAction Technology 1-7
- Ability to Perform ActiveUpdates at Random Intervals 1-7

Support for Multiple Update Sources 1-8
HTTPS (SSL) Support 1-8
An Improved User Interface 1-8
Remote Installation 1-9
One Binary Package for All Supported Linux Distributions 1-9
Support for Wildcards with Exclusion Directory 1-9

What's New in This Release 1-10

Understanding How ServerProtect Works 1-10

Exploring ServerProtect Scanning Technologies 1-12
Pattern Matching 1-12
MacroTrap 1-12
How MacroTrap Works 1-13
Compressed File Scanning 1-13
Compressed File Scan Limit 1-13

Chapter 2: Getting Started with ServerProtect

Accessing the ServerProtect Web Console 2-2

Setting Logon Password 2-3

Bypassing Password Checking for Local Logon 2-3

Logging off from the Web Console 2-4

Things to Remember About the Web Console 2-4

Starting and Stopping ServerProtect 2-5

Starting ServerProtect 2-5
Stopping ServerProtect 2-6

Configuring Startup Settings 2-6

Viewing Summary Information 2-7

Managing ServerProtect From Trend Micro Control Manager 2-8

Registering ServerProtect to Control Manager Using the Web Console 2-9
Registering ServerProtect to Control Manager Using the CMconfig tool 2-12

Initiating Automatic Update on Control Manager 2-14

Chapter 3: Configuring and Performing Scans with ServerProtect

Types of Scanning 3-2
Configuring Real-Time Scan 3-3
Configuring Scheduled Scan 3-4
Invoking Scheduled Scan from the Command Line 3-5
Stopping a Scheduled Scan 3-5
Invoking Manual Scan (Scan Now) 3-6
Configuring Scan Settings 3-7
Configuring Scanning Directories 3-8
Specifying Files to Scan 3-9
Scanning Compressed Files 3-12
Specifying Actions on Infected Files 3-13
Exclusion List 3-15
Using Wildcard Characters 3-16
Specifying the Quarantine Directory 3-17
Specifying the Backup Directory Location 3-18

Chapter 4: Update

About ActiveUpdate 4-2
Component Updates 4-2
Specifying a Download Source 4-3
Configuring Proxy Server Settings 4-4
World Virus Tracking and License Update 4-4
Component Update 4-5
Manual Update 4-7
Performing a Manual Update from the Summary Screen . 4-7
Performing a Manual Update from the Manual Update Screen 4-8

Scheduled Updates 4-9

Chapter 5: Logs

Types of Logs 5-2

Viewing Scan Results in Logs 5-2

Using the Scan Now Complete Window 5-3
Using the Log Screens in the Web Console 5-3

Specifying the Log Directory Location 5-7

Deleting Logs 5-7

Automatically Deleting Logs 5-7
Manually Deleting Logs 5-8

Configuring Notifications 5-10

Setting Alert Events 5-10
Updating Alert Settings 5-10
Creating Custom Notifications 5-13
Specifying Notification Recipients 5-13
Enabling SMTP Mail Notification 5-14
Configuring Recipient Settings 5-15
Enabling SNMP Notification 5-16

Chapter 6: Troubleshooting

Troubleshooting Tips 6-2

Default Password 6-2
Web Console Rejects All Passwords 6-2
Automatic Component Update 6-2
System Logs Related to ServerProtect 6-2

Debug Logging 6-3

Debug Levels 6-3
Enabling Debug Logging 6-4
Disable Debug Logging 6-5

Chapter 7: Technical support

Troubleshooting resources 7-2
Using the support portal 7-2
Threat encyclopedia 7-2
Contacting Trend Micro 7-3
Speeding up the support call 7-3
Sending suspicious content to Trend Micro 7-4
Email Reputation Services 7-4
File Reputation Services 7-4
Web Reputation Services 7-5
Other resources 7-5
Download center 7-5

Appendices

Appendix A: Configuration Commands

Accessing ServerProtect Man Pages A-2
Understanding tmsplx.xml A-2
Scan Group Keys A-4
Scan Group Key Set A-4
ActiveUpdate Group Keys A-16
ActiveUpdate Group Key Set A-16
SOURCEINFO Group Keys A-19
SOURCEINFO Group Key Set A-19
DESTINFO Group Key A-22
Notification Group Keys A-22
Notification Group Key Set A-22
Configuration Group Keys A-27
Configuration Group Key Set A-27
GUIPassword Group Keys A-30
Logs Group Keys A-30
Logs Group Key Set A-31

Registration Group Keys A-32
Registration Group Key Set A-32
Backing Up and Verifying the Configuration File A-35
Using RemoteInstall.conf A-35
Using splxmain A-37
Using splx A-41
Using splxcore A-42
Using splxhttpd A-42
Using splxcomp A-43
Using CMconfig A-44
Apache Configuration File A-45
Apache Log Files A-45

Appendix B: Glossary of Terms

Index

Index IN-1

Preface

Preface

Welcome to the Trend Micro™ ServerProtect for Linux Administrator's Guide. 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 for Linux Documentation on page 2*
- *Audience on page 2*
- *Document Conventions on page 3*

ServerProtect for Linux Documentation

The product documentation consists of the following:

- **Online Help**: Web-based documentation that is accessible from the product console

  The Online Help contains explanations about ServerProtect for Linux features.

- **Linux Man pages**: ServerProtect for Linux provides man pages for the `splxmain`, `splx`, `tmsplx.xml`, `RemoteInstall`, and `CMconfig`. See *Accessing ServerProtect Man Pages on page A-2* for more information.

- **Administrator's Guide**: PDF documentation that discusses getting started information and product management

- **Readme File**: Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

- **Knowledge Base**: Contains the latest information about all Trend Micro products. Other inquiries that were already answered area also posted and a dynamic list of the most frequently asked question is also displayed.

  https://success.trendmicro.com/

Note

Trend Micro recommends checking the corresponding link from the Update Center (http://docs.trendmicro.com/en-us/home.aspx) for updates to the documentation.

Audience

The 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 ServerProtect for Linux documentation uses the following conventions:

TABLE 1. Document 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 or new technology components
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, `C:\Program Files\<file_name>` can be `C:\Program Files\sample.jpg`.
Note	Provides configuration notes or recommendations
Tip	Provides best practice information and Trend Micro recommendations
WARNING!	Provides warnings about activities that may harm computers on your network

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:

- *Main Features on page 1-2*
- *What's New in This Release on page 1-10*
- *Understanding How ServerProtect Works on page 1-10*

Main Features

The following are main features of ServerProtect for Linux:

Managing ServerProtect Through Trend Micro Apex Central or Trend Micro Control Manager

Trend Micro Apex Central™ (formerly known as Trend Micro Control Manager™) is a central management console that manages Trend Micro products and services, including ServerProtect for Linux. When registered to Apex Central / Control Manager, ServerProtect can make use of features such as:

- Reports are available from Apex Central / Control Manager.
- Outbreak Prevention Services (for file blocking). See *Outbreak Prevention Services on page 1-4*.

Note

All the Control Manager features and settings mentioned in this document are applicable to Apex Central.

ServerProtect for Linux supports the following Apex Central / Control Manager versions:

- Apex Central 2019 or later
- Control Manager 7.0 or later

Reports Available from Apex Central / Control Manager

The following reports are available from Apex Central / Control Manager:

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

The Apex Central / Control Manager server consolidates these reports from log data, so these reports are available only when managing ServerProtect from Apex Central / 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 3-15* 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 Apex Central / 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 Apex Central / 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: Apex Central / Control Manager.

With OPS, Apex Central / 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 *Using splxmain on page A-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.

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

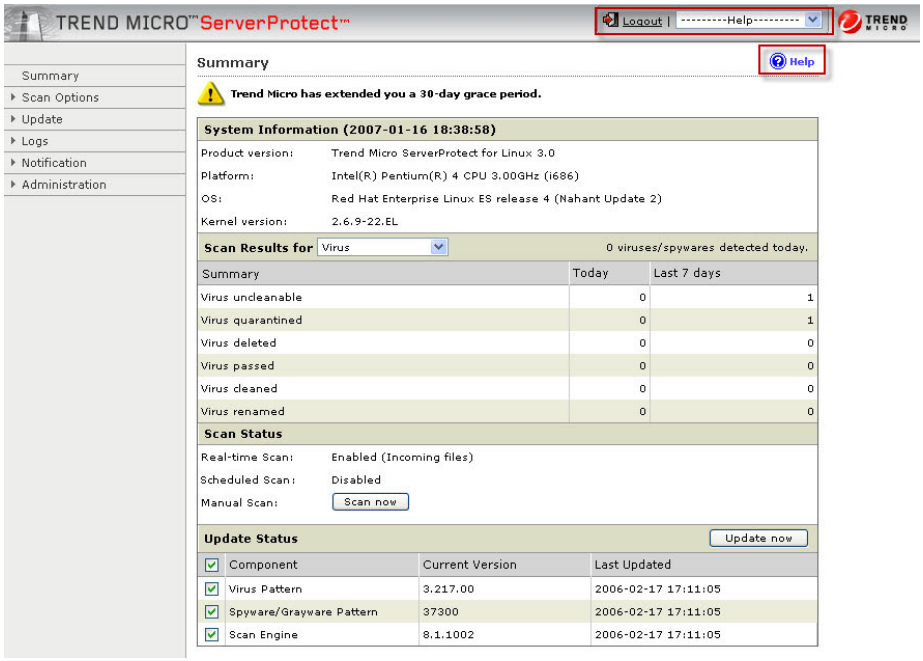


FIGURE 1-1. Enhanced user interface

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 ServerProtect for Linux, the following new features are available in version 3.0:

Feature	Description
Support for New Platforms	In this release, supported platforms are based on the Linux kernel 6.12. The supported platform is: SUSE Linux Enterprise Server 16

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.

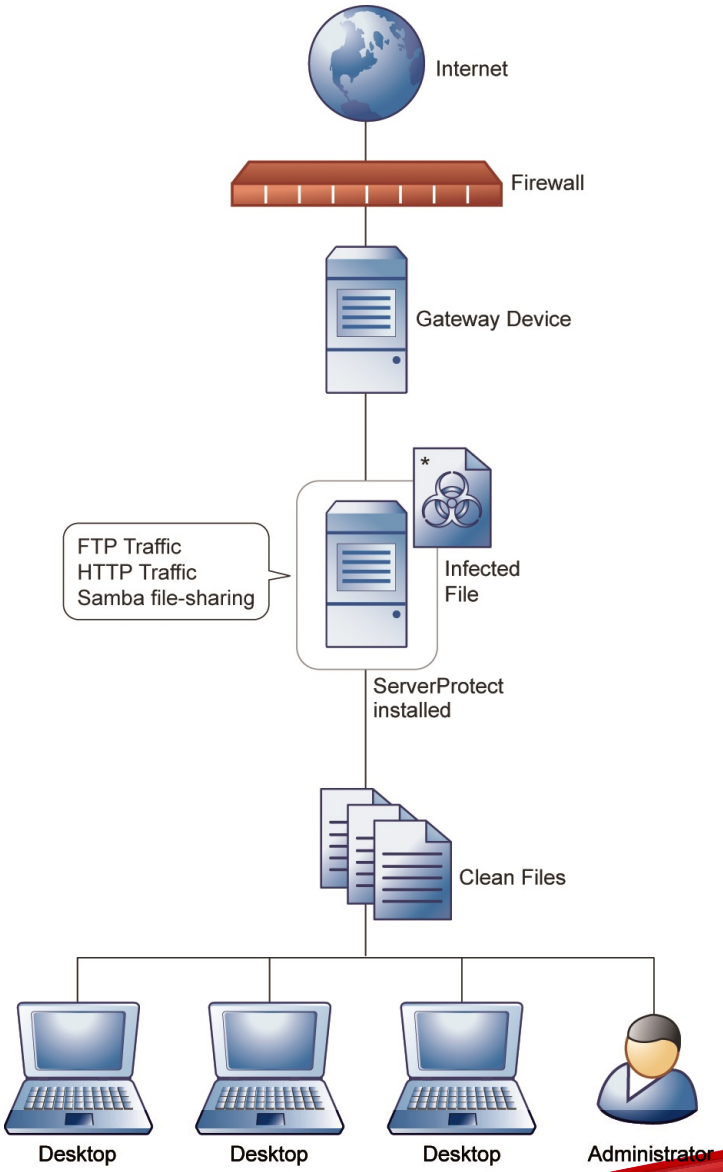


FIGURE 1-2. How Se

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.

Chapter 2

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 on page 2-2*
- *Setting Logon Password on page 2-3*
- *Logging off from the Web Console on page 2-4*
- *Things to Remember About the Web Console on page 2-4*
- *Starting and Stopping ServerProtect on page 2-5*
- *Configuring Startup Settings on page 2-6*
- *Viewing Summary Information on page 2-7*
- *Managing ServerProtect From Trend Micro Control Manager on page 2-8*

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:

- A supported Web browser

Procedure

1. Log on as `root`.
2. Access the Web console.
   - 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 on page A-37* for more information.

If you are using Internet Explorer 7.0 or later, 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.

Procedure

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.

Procedure

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 (see *Starting and Stopping ServerProtect on page 2-5*).
- To refresh a Web console screen, use your browser's Refresh option.
- The Web console automatically logs you out after 1,200 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 Apex Central / Control Manager

Starting and Stopping ServerProtect

Note

By default, ServerProtect starts whenever you turn on the server hosting it. To change this setting, see *Configuring Startup Settings on page 2-6*.

Starting ServerProtect

Task	Step

Starting 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 ~]#`

Stopping ServerProtect

Task	Step

Stopping 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 ~]#`

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:

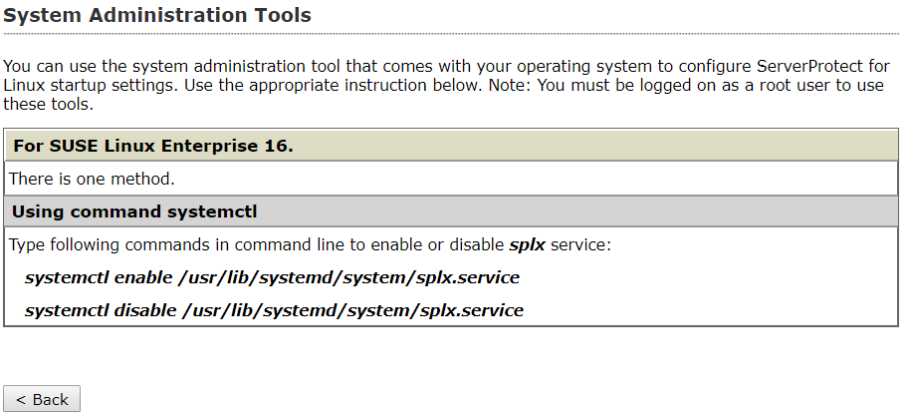


FIGURE 2-1. Administration: Startup Settings

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. See **`MaxRetrieveCount`** in *Logs Group Key Set on page A-31* 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 Trend Micro Control Manager

Note

Trend Micro Control Manager are now renamed Trend Micro Apex Central. All the Control Manager features and settings mentioned in this document are applicable to Apex Central.

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
- *Using the ServerProtect Web console on page 2-9*

- *Using the CMconfig tool on page 2-12*

Registering ServerProtect to Control Manager Using the Web Console

Procedure

1. Log on to the Web console.
2. Click **Administration** > **Control Manager Settings**.

The **Control Manager Settings** screen displays.

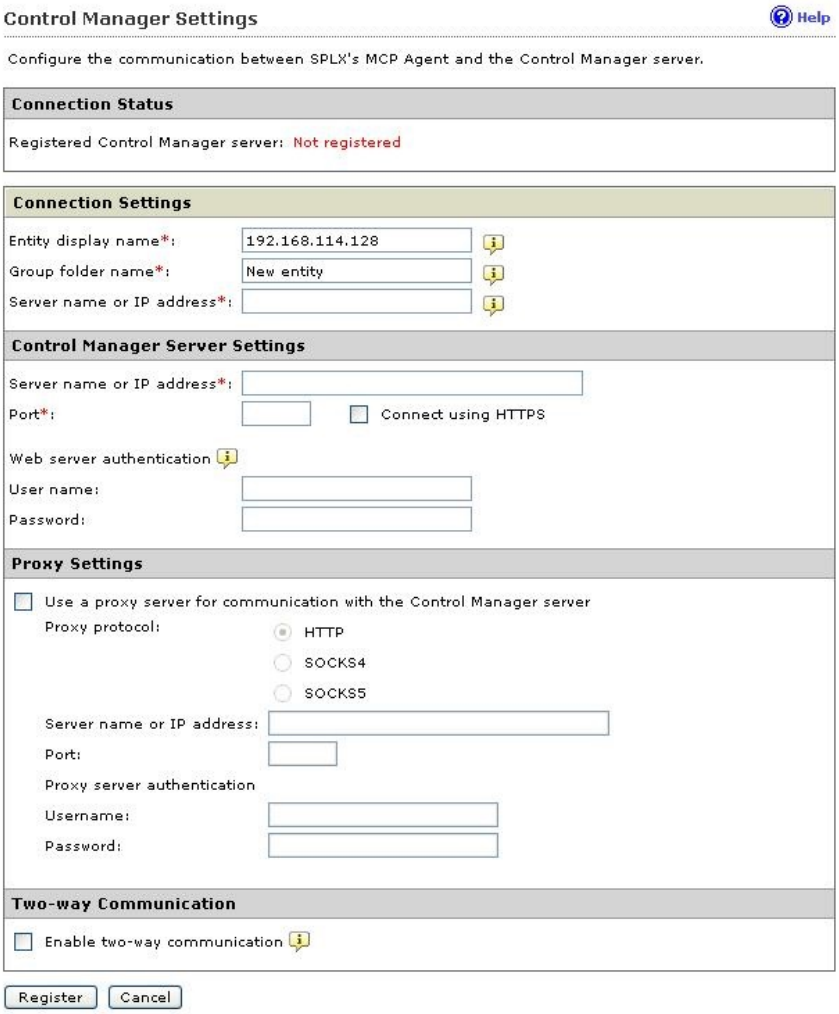


FIGURE 2-2. Control Manager

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.

Registering ServerProtect to Control Manager Using the CMconfig tool

Procedure

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.

Procedure

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.

Note

To learn more information about managing products in Control Manager, refer to the Apex Central 2019 documentation.

Chapter 3

Configuring and Performing Scans with ServerProtect

This chapter discusses the following topics:

- *Types of Scanning on page 3-2*
- *Configuring Real-Time Scan on page 3-3*
- *Configuring Scheduled Scan on page 3-4*
- *Invoking Manual Scan (Scan Now) on page 3-6*
- *Configuring Scan Settings on page 3-7*
- *Exclusion List on page 3-15*
- *Specifying the Quarantine Directory on page 3-17*
- *Specifying the Backup Directory Location on page 3-18*

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 Trend Micro 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.

The following sections show 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:

Procedure

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.

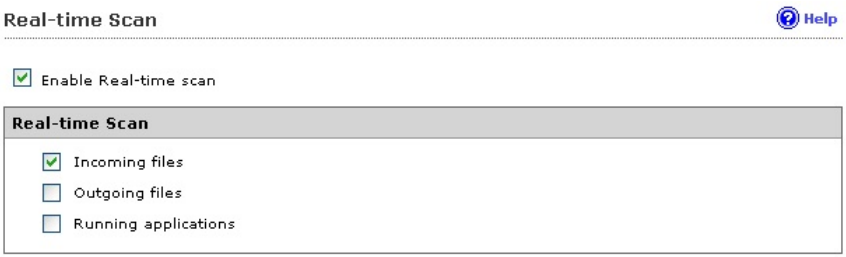


FIGURE 3-1. Activating and configuring real-time scan

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, see *Configuring Scan Settings on page 3-7*.

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.

Procedure

1. Configure a scheduled scan.
   a. Click **Scan Options** > **Scheduled Scan** on the left menu.
   b. Select the **Enable Scheduled Scan** check box.
   c. Click **Save** to apply the setting.

FIGURE 3-2. Activating and configuring scheduled scan

2. Configure scan frequency for a scheduled scan.
   a. Click **Scan Options** > **Scheduled Scan** on the left menu.
   b. 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.
   c. Click **Save** to apply the settings. To configure other scanning settings, see *Configuring Scan Settings on page 3-7*.

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, see *Configuring Scan Settings on page 3-7*.

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**.

Task	Description
Start scanning 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 3-15*. 3. Click **Save & Scan**. A confirmation window displays. 4. Click **OK** to begin the scan. The scan progress window appears showing the status of the scan. **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.

Running 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:	1. Click **Stop Scanning** in the scan progress window. 2. Run the following command: `./splxmain -n` 3. 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

Procedure

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.

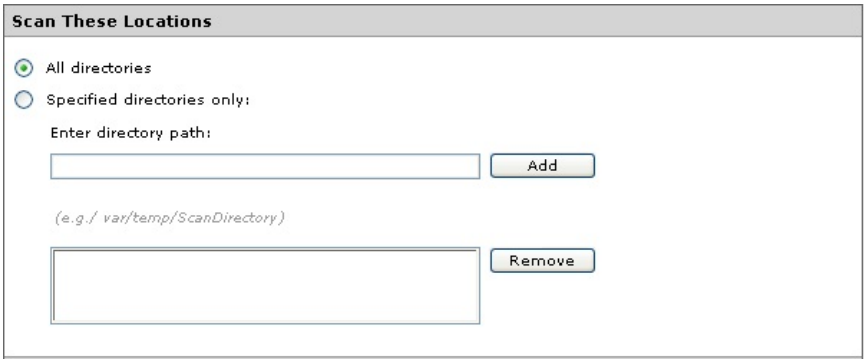


FIGURE 3-3. Select directories to scan

- **All directories**: scans all directories, except those included in the Exclusion List. For additional information, see *Exclusion List on page 3-15*.
- **Specified directories only**: limits the scan to the directories and subdirectories that you specify. To do so:

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

Note

The directory path names are case-sensitive.

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

c. 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, select the directory for removal in the **Scan these directories** list and click **Remove** to remove the selected entry. 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.

Procedure

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.

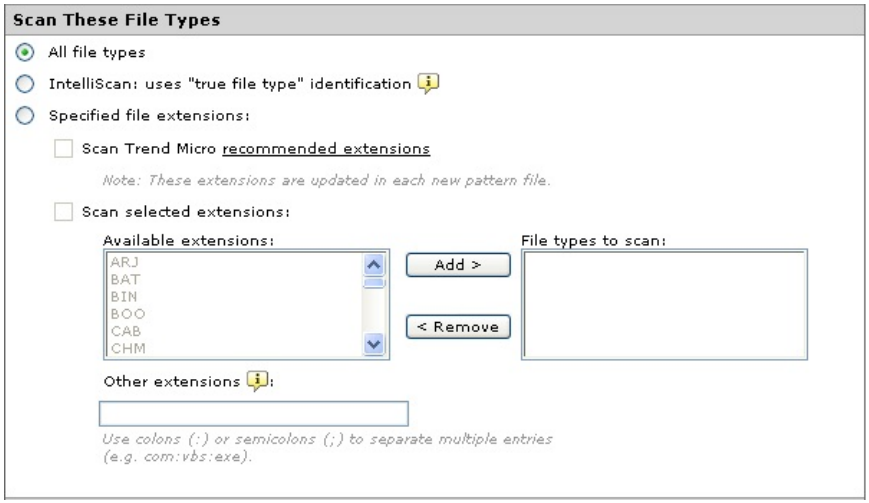


FIGURE 3-4. Selecting file types to scan

- **All file types**: Scans all files, except for those specified in the Exclusion List screen (see *Exclusion List on page 3-15*).
- **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.
  - **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:

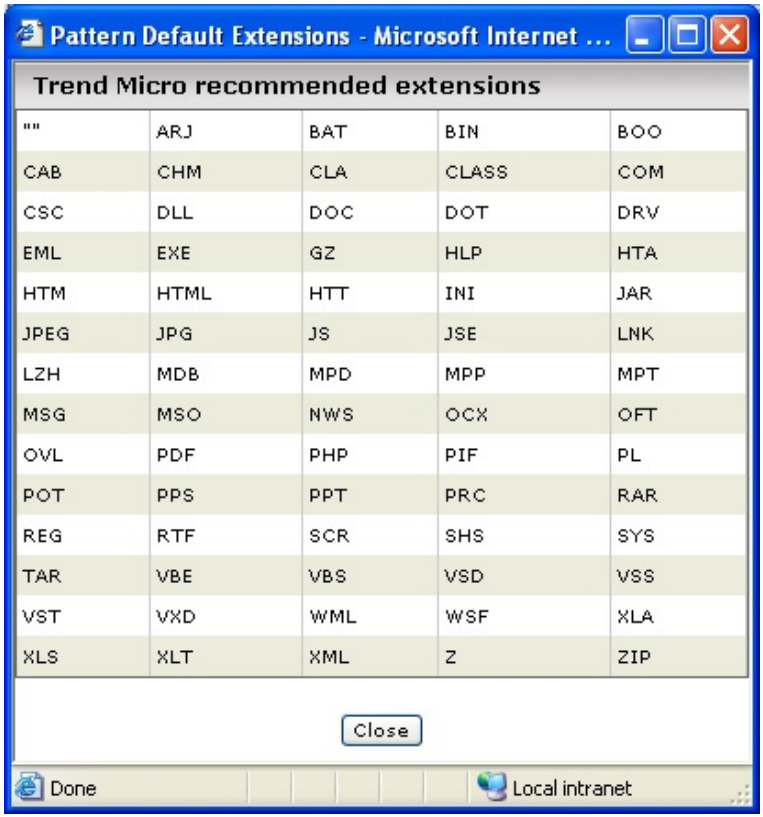


FIGURE 3-5. Trend Micro recommended extensions for file scanning

- **Scan selected extensions**. You can specify extensions from a list of extensions. To do so:

  a. Select the extension from the **Select extensions...** list.

  b. Click **Add >** to add the extension to the **File Types to scan** list.

c. 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**.

Note

To remove extensions, select the extension to be excluded from scanning in the **File types to scan** list, click **< Remove** to remove the extension, and click **Save**.

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.

Procedure

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.

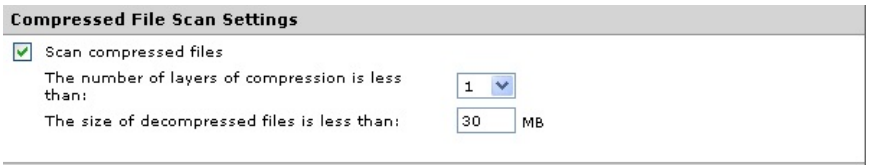


FIGURE 3-6. Compressed file scanning

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.

Procedure

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.

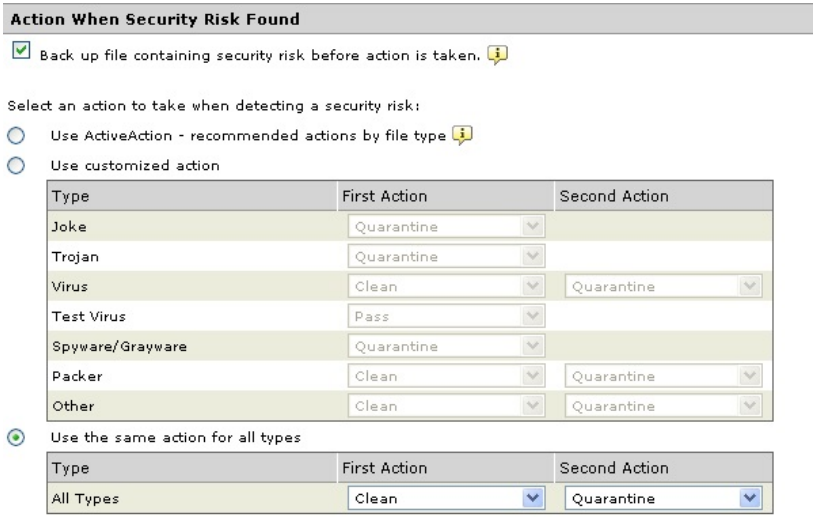


FIGURE 3-7. Specify scan actions

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.

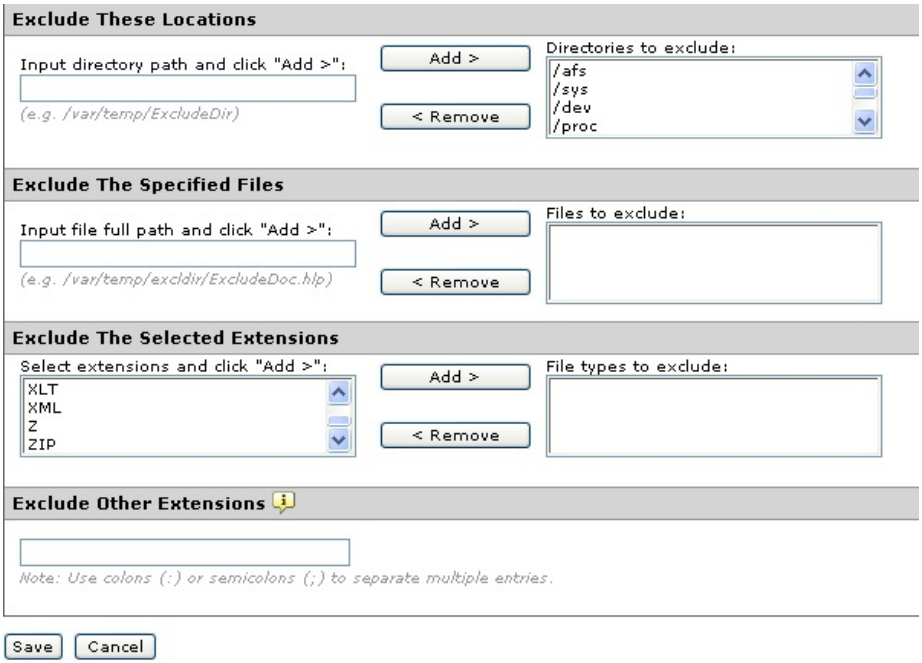


FIGURE 3-8. Exclusion list

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 theServerProtect 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.

Procedure

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.

Procedure

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 on page 4-2*
- *Configuring Proxy Server Settings on page 4-4*
- *Manual Update on page 4-7*
- *Scheduled Updates on page 4-9*

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`

Procedure

1. Configure *manual on page 4-7* or *scheduled on page 4-9* update.
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
   - **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.

Feature	Reference
World Virus Tracking License update	For details, see *World Virus Tracking and License Update on page 4-4*.
Component update	For details, see *Component Update on page 4-5*.

World Virus Tracking and License Update

Procedure

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**.

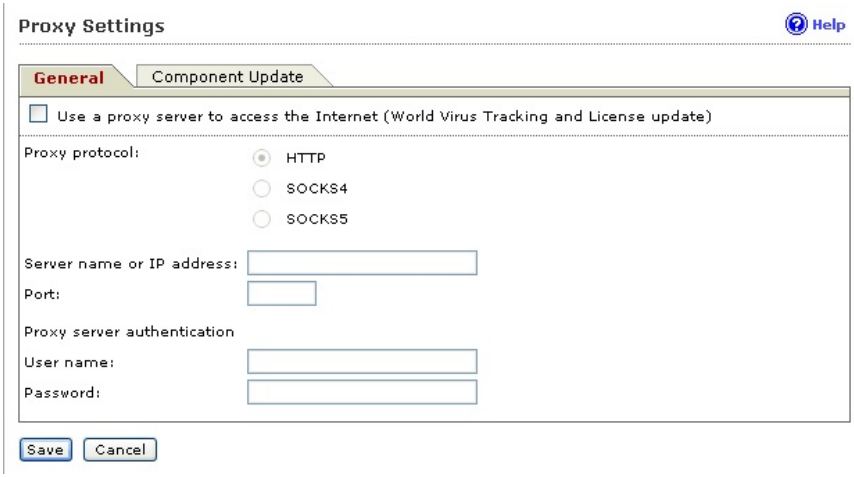


FIGURE 4-1. Proxy Settings General screen

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.

Component Update

Procedure

1. Click **Administration** > **Proxy Settings** > **Component Update**.

The **Component Update** screen displays.

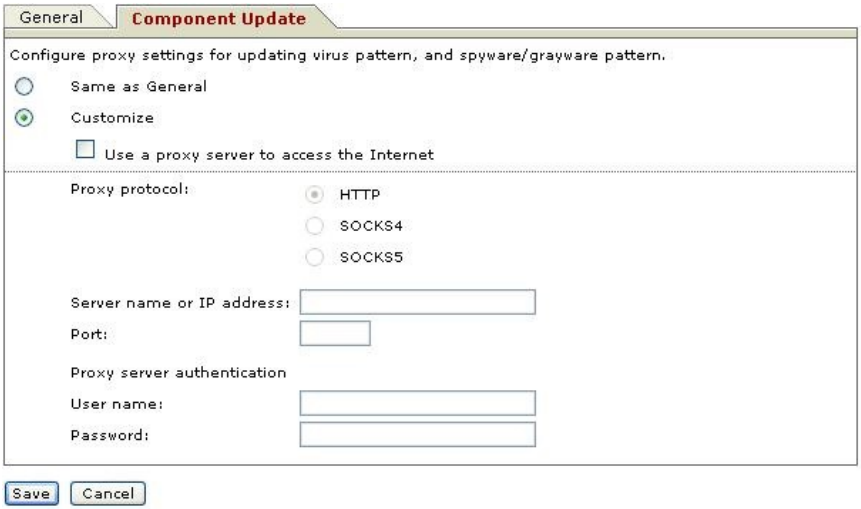


FIGURE 4-2. Proxy Settings Component Update screen

2. Select either of the following options.

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

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

        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 3.

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

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

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

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

3. Click **Save**.

Tip

To set the proxy password from the command prompt, see *Using splxmain on page A-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** screen. For details, see *Performing a Manual Update from the Summary Screen on page 4-7*.
- Click **Update Now** from the **Manual Update** screen. For details, see *Performing a Manual Update from the Manual Update Screen on page 4-8*.

Performing a Manual Update from the Summary Screen

Procedure

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**.

Performing a Manual Update from the Manual Update Screen

Procedure

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. See *Specifying a Download Source on page 4-3*.

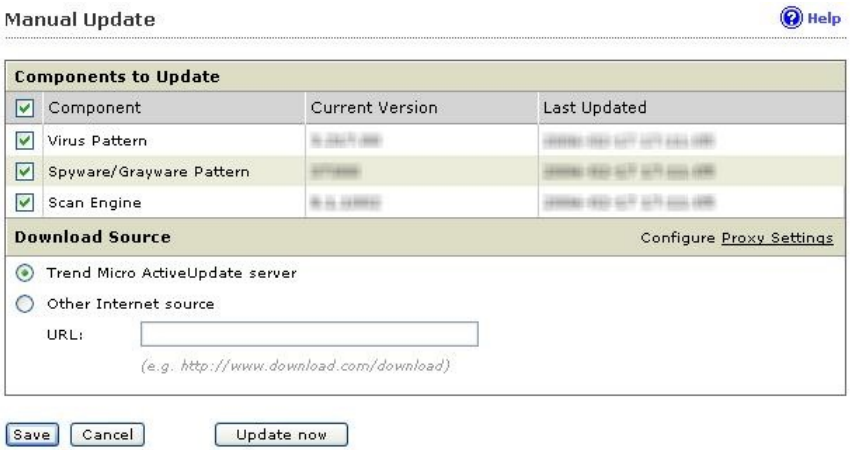


FIGURE 4-3. Manual Update screen

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.

Procedure

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. See *Specifying a Download Source on page 4-3* for more information.

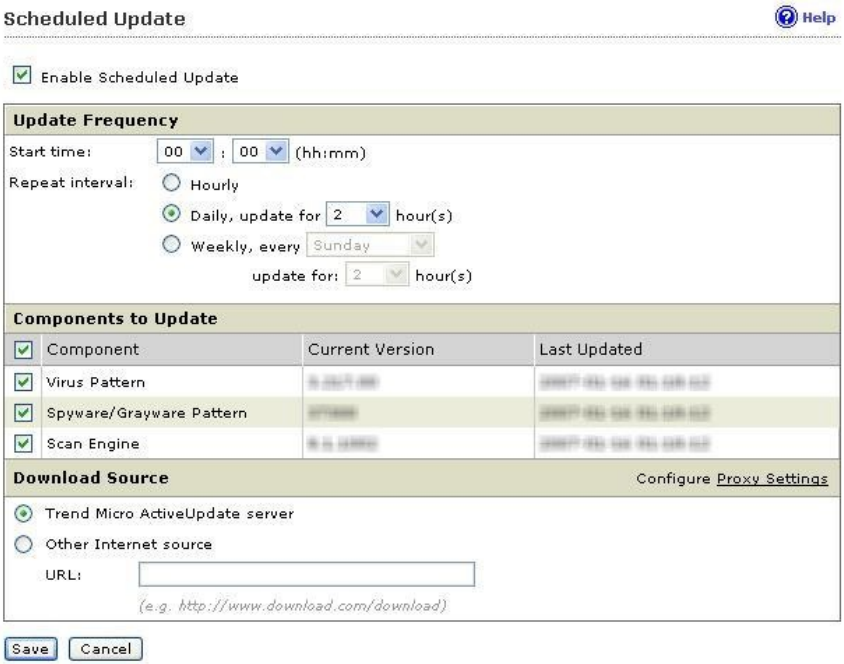


FIGURE 4-4. Scheduled Update screen

8. Click **Save**.

Chapter 5

Logs

This chapter discusses the following topics:

- *Types of Logs on page 5-2*
- *Viewing Scan Results in Logs on page 5-2*
- *Specifying the Log Directory Location on page 5-7*
- *Deleting Logs on page 5-7*
- *Configuring Notifications on page 5-10*

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 in 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.

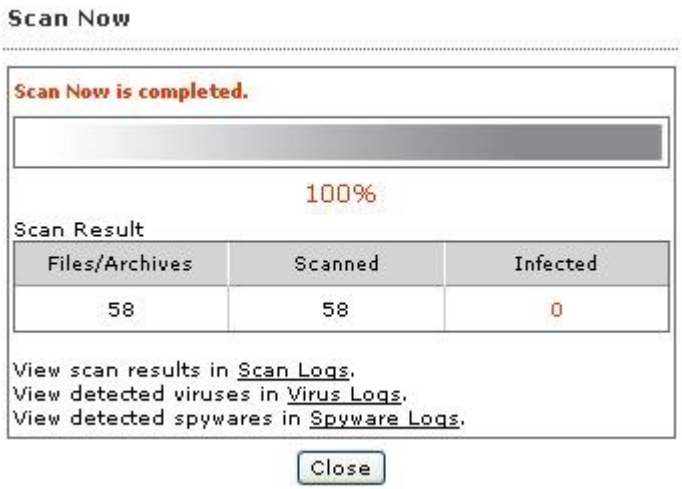


FIGURE 5-1. Scan Now complete window

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

Procedure

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.

   - **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" in *Logs Group Key Set on page A-31* for more information.

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

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

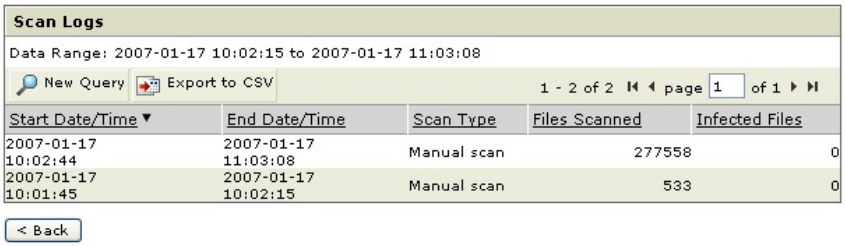


FIGURE 5-2. Scan log example

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

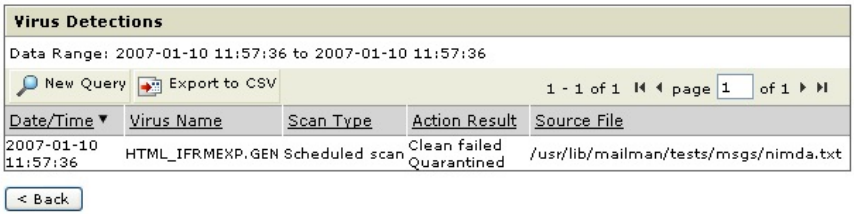
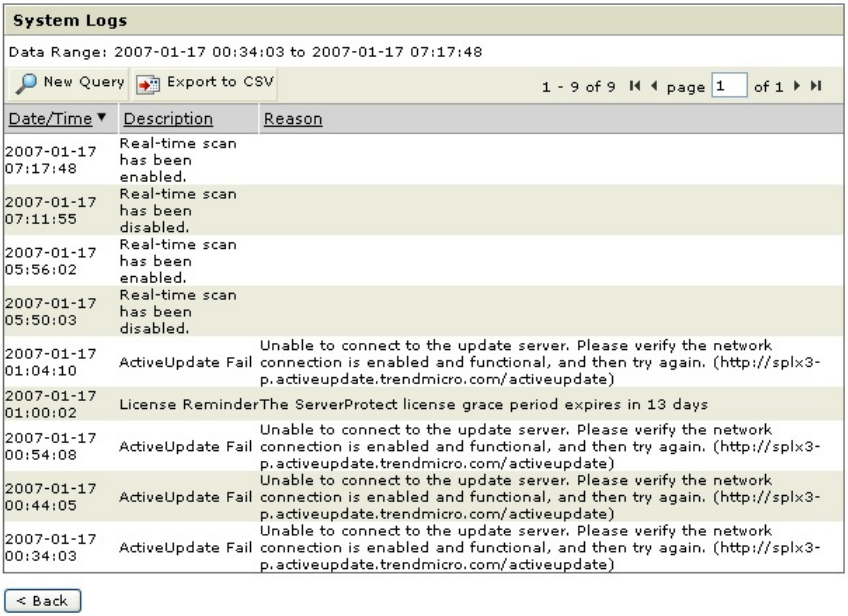


FIGURE 5-3. Virus log example

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 (). 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
```

Procedure

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.

Procedure

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.

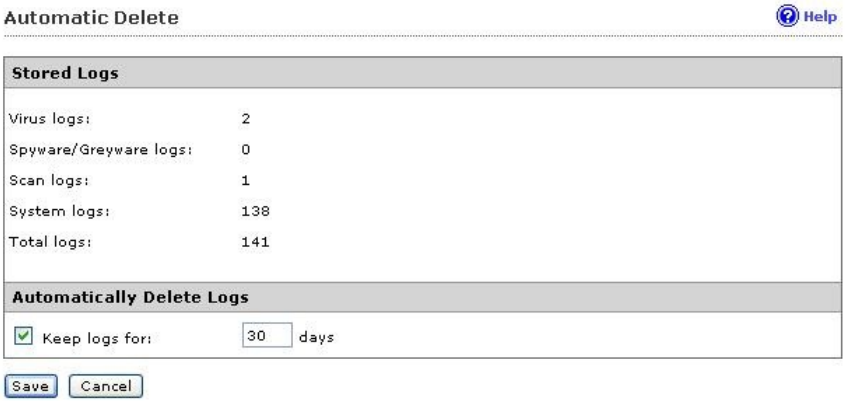


FIGURE 5-5. Automatic Delete

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

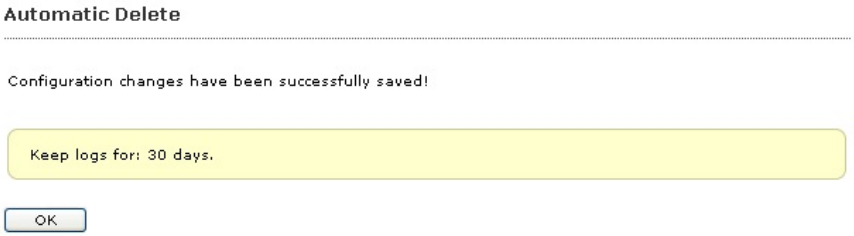


FIGURE 5-6. Automatic Delete Settings Saved

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.

Procedure

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.

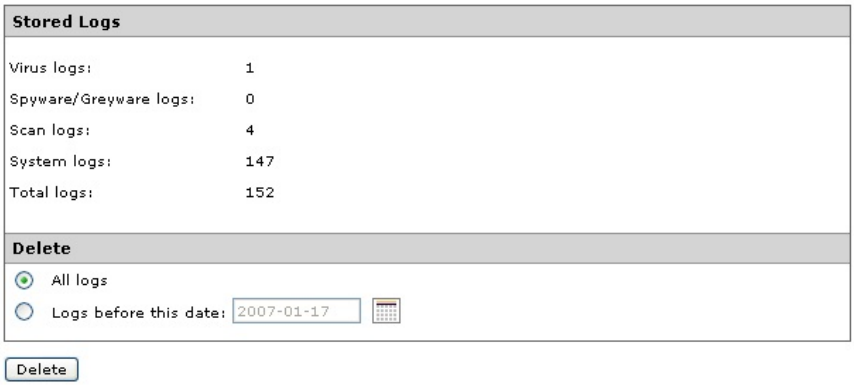


FIGURE 5-7. Manual Delete

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.

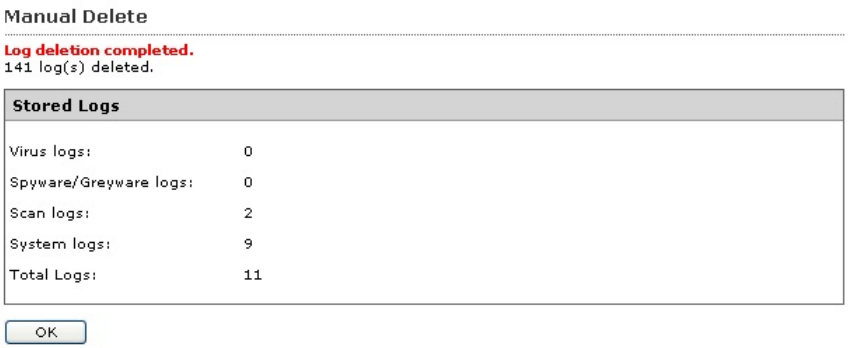


FIGURE 5-9. Manual Delete Result

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

Updating Alert Settings

Procedure

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.

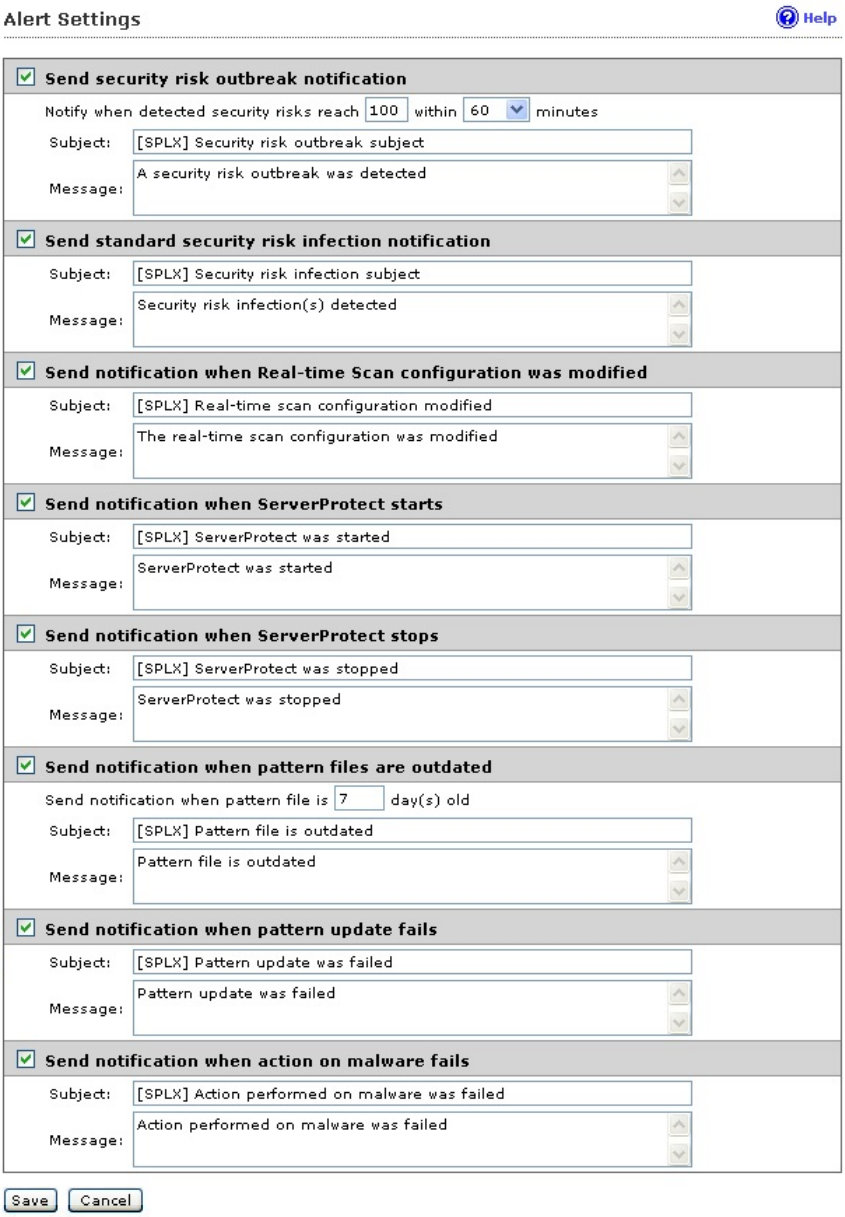


FIGURE 5-10. Notification Alert Messages

Creating Custom Notifications

Procedure

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

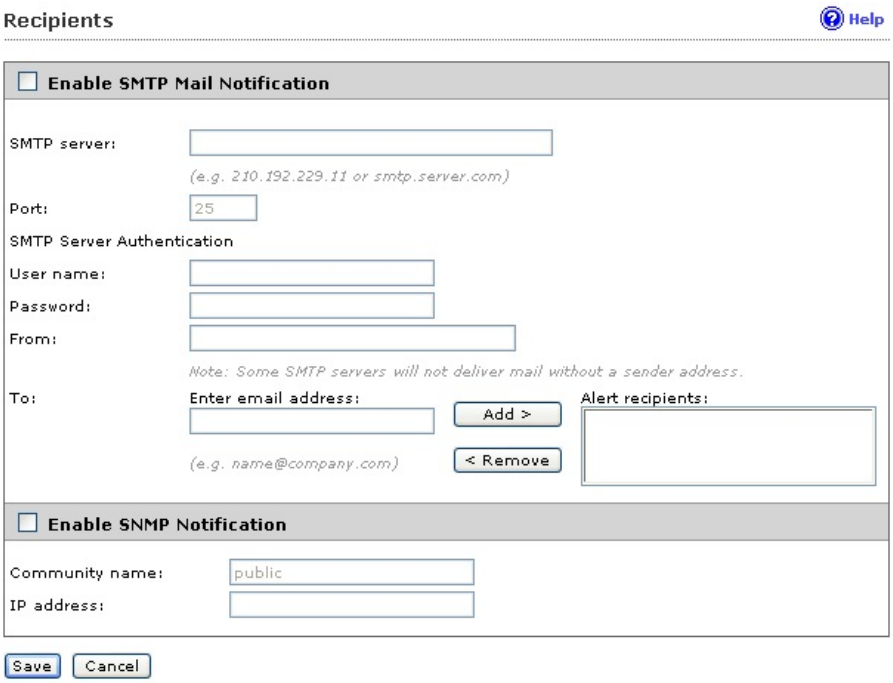


FIGURE 5-11. Notification Recipients

Enabling SMTP Mail Notification

Procedure

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**.

Configuring Recipient Settings

Procedure

1. Click **Notification** > **Recipients** from the left menu.
2. Configure recipient settings.
   - Add a recipient address:
     a. Type the recipient's full email address in the **Enter email address** field, for example:

        `yourname@yourCompany.com`

     b. Click **Add >** to add the entry to the **Alert Recipients** list.
     c. Click **Save**.
   - Modify recipient settings:
     a. Select an address from the **Alert Recipients** list.
     b. Make the appropriate modifications, then click **Save**.
   - Remove a recipient address:
     a. Select an address from the **Alert Recipients** list.
     b. Click **< Remove** to remove the selected entry from the recipients list.
     c. Click **Save** to apply the changes.

Enabling SNMP Notification

Procedure

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

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

- *Troubleshooting Tips on page 6-2*
- *Debug Logging on page 6-3*

Troubleshooting Tips

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 A-42*.

- 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 2-14*.

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

Debug Levels

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

TABLE 6-1. Debug levels editable with tmsplx.xml

VALUE	KERNEL DEBUGGING (KERNELDEBUGLEVEL)	USER DEBUGGING (USERDEBUGLEVEL)	TMCM DEBUGGING (CONTROLMANAGER DEBUG)
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

Value	Kernel Debugging (KernelDebugLevel)	User Debugging (UserDebugLevel)	TMCM Debugging (ControlManager Debug)
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

- `UserDebugLevel` does not control output from startup scripts. They will always be logged regardless of the `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 `rsyslog.conf` to enable ServerProtect debug logging.

Procedure

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 `rsyslog.conf` to restore your original settings. After modifying the `rsyslog.conf` file, restart the rsyslog 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/rsyslog.conf`.

- To direct all ServerProtect user debug logs to , include the following line in `rsyslog.conf`:

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

2. Save and close the configuration file.

3. Restart ServerProtect service:

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

Disable Debug Logging

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

Procedure

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 `rsyslog.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/rsyslog.conf`

4. Restart ServerProtect service:

   `/etc/init.d/splx restart`

Note

To prevent Linux file operation errors, restart the ServerProtect service before you restart rsyslog.

Chapter 7

Technical support

Learn about the following topics:

- *Troubleshooting resources on page 7-2*
- *Contacting Trend Micro on page 7-3*
- *Sending suspicious content to Trend Micro on page 7-4*
- *Other resources on page 7-5*

Troubleshooting resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the support portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to https://success.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

   Tip

   To submit a support case online, visit the following URL:

   https://success.trendmicro.com/en-US/contactus/

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	• https://www.trendmicro.com • https://success.trendmicro.com/en-US/contactus/

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  https://docs.trendmicro.com

Speeding up the support call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information

- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending suspicious content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://servicecentral.trendmicro.com/en-us/ers/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

https://success.trendmicro.com/en-US/solution/KA-0001177

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

https://success.trendmicro.com/en-US/solution/KA-0002449

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

https://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download center

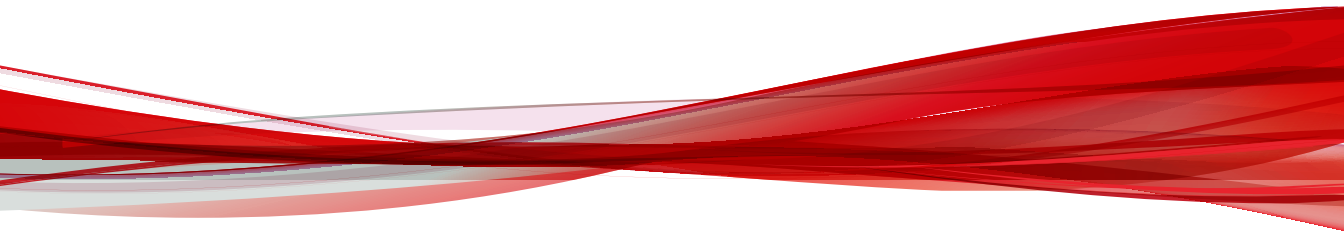
From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

https://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Appendices

Appendices



Appendix A

Configuration Commands

This appendix provides additional information about configuring ServerProtect using commands.

This appendix discusses the following topics:

- *Accessing ServerProtect Man Pages on page A-2*
- *Understanding tmsplx.xml on page A-2*
- *Using RemoteInstall.conf on page A-35*
- *Using splxmain on page A-37*
- *Using splx on page A-41*
- *Using splxcore on page A-42*
- *Using splxhttpd on page A-42*
- *Using splxcomp on page A-43*
- *Using CMconfig on page A-44*
- *Apache Configuration File on page A-45*
- *Apache Log Files on page A-45*

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

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 and CentOS. 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.

Scan Group Key Set

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.

RealtimeExcludeCommand

Use this key to exclude certain commands from scanning. Type the full name of the processes, and then separate them with a colon (:).

For example, to exclude the vsapiapp and splxmain in the Real-time Scan process, type the following:

```
<P Name="RealtimeExcludeCommand" Value="vsapiapp:splxmain"/>
```

RealtimeNotScanSize, OnDemandNotScanSize

Use these keys to set the Single file size (megabytes) limit for manual/ schedule scan and real-time scan.

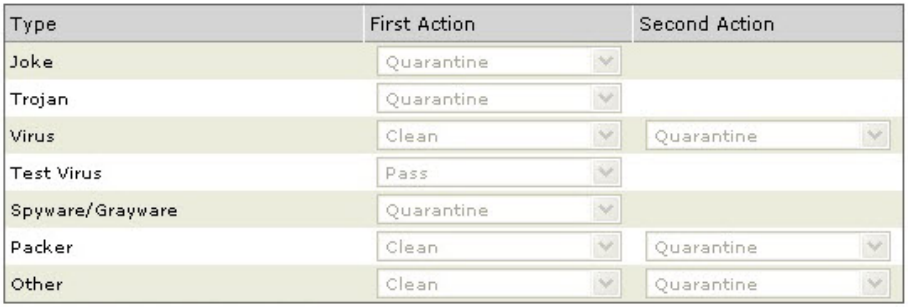
For example, to set the single file size limit for Real-time Scan, type the following:

```
<P Name=”OnDemandNotScanSize” Value=”10”/>
```

After executing this command, all files over 10MB in size will not be scanned.

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

FIGURE A-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.

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

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

The following values apply:

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

Therefore, the default custom settings are as follows:

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

Note

When the RealtimeCustomizedAction, ScheduledCustomizedAction, ManualCustomizedAction, RealtimeAllTypesAction, ScheduledAllTypesAction and ManualAllTypesAction keys are set to zero, ServerProtect automatically uses ActiveAction for Real-time Scan, Scheduled Scan, and Manual Scan.

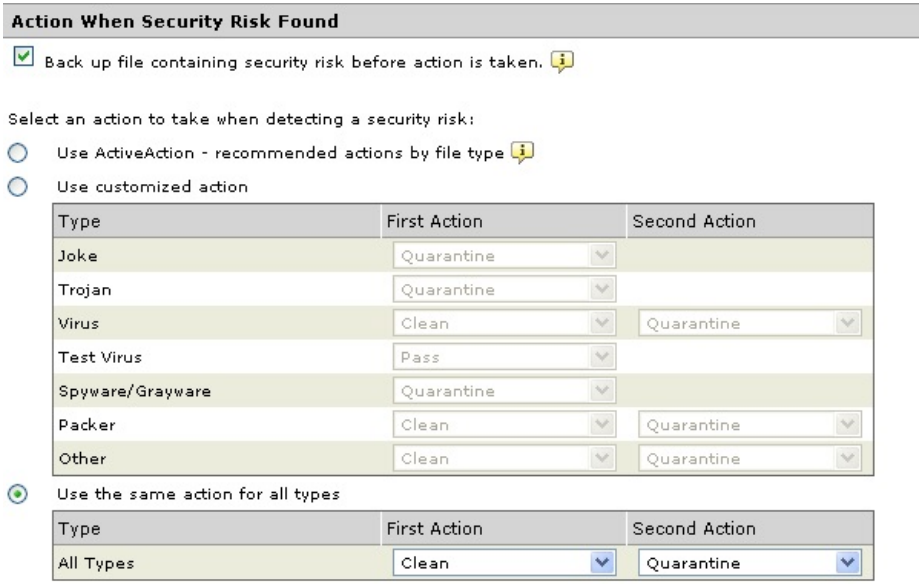


FIGURE A-3. ActiveAction is enabled when settings for Customized and All Types are set to 0

RealTimeScanArchived, ScheduledScanArchived, ManualScanArchived

This key is not used.

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.

ActiveUpdate Group Key Set

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.

SOURCEINFO Group Key Set

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 A-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

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.

Notification Group Key Set

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.

Configuration Group Key Set

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 rsyslog.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 `rsyslog.conf` file (`/var/log/messages` by default). See *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 *Debug Levels on page 6-3*.

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.

Logs Group Key Set

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.

Registration Group Key Set

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.

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.

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

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.

KEY	DEFAULT VALUE	DESCRIPTION
XMLvalidatorPath	config/xmlvalidator	Indicates the XMLvalidator script path. Used for configuration file deployment.
XMLdeployerPath	config/xmldeployer	Indicates the XMLdeployer program file path. Used for configuration file deployment.
KHMPath	KHM.module/RHEL4/splxmod-2.6.9-22.0.2.ELsmp.o	Indicates KHM file path. Used for KHM deployment. Limit is one KHM file per KHM deployment.
ConnectTimeOut	30	Specifies the timeout (in seconds) used when connecting to the ssh server, instead of using the default system TCP timeout. Used only when the target is down or unreachable, not when it refuses the connection.
ConnectRetry	2	Used to retry frequency of ssh connection.
AliveInterval*	30	Sets a timeout interval in seconds after which if no data has been received from the server, ssh will send a message through the encrypted channel to request a response from the server. This option applies to protocol version 2 only. See `ssh_config` man page, keyword **ServerAliveInterval**.
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, keyword **ServerAliveCountMax**.
ResponseTimeOut	120	The time allowed for process client response.

KEY	DEFAULT VALUE	DESCRIPTION

Debug	0	Possible values are 0 (disable debug mode) and 1 (enable). If you enable debug mode, modify `rsyslog.conf` file to set an entry as follows:
		1. Set an entry as below for ServerProtect in rsyslogd's configuration file, `/etc/rsyslog.conf`.
		In `/etc/rsyslog.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 `rsyslog`
		3. Set `rsyslogd` 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.

Note

Trend Micro recommends keeping 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

variousServerProtect 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.

`-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.

-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` in *Logs Group Key Set on page A-31*.

-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
```

-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.

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/
```

Appendix B

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

Term	Explanation
?	Character that can be used as a wildcard when specifying directories to be scanned or excluded from scanning.
access (verb)	To read data from or write data to a storage device, such as a computer or server.
access (noun)	Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.
action	The operation to be performed when a virus or other malware has been detected. Actions typically include clean, quarantine, delete, or pass (deliver/transfer anyway). Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your software after completion of the registration process. Trend Micro products will be installed as an evaluation version.Activate during installation or after installation (in the management console) in the Product License screen.

TERM	EXPLANATION
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.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption.

Term	Explanation
ELF	Executable and Linkable Format—An executable file format for Unix and Linux platforms.
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.
EUC-KR	A method of 8-bit character encoding used for the Korean language. See the following Web site for more information: http://en.wikipedia.org/wiki/EUC-KR
EXE file infector	An executable program will a .exe file extension.
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
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.

TERM	EXPLANATION
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.
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.

TERM	EXPLANATION
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.

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.

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.

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.

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.

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.

Index

S

support
resolve issues faster, 7-3

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736

www.trendmicro.com

Item Code: SPEM310096/260302