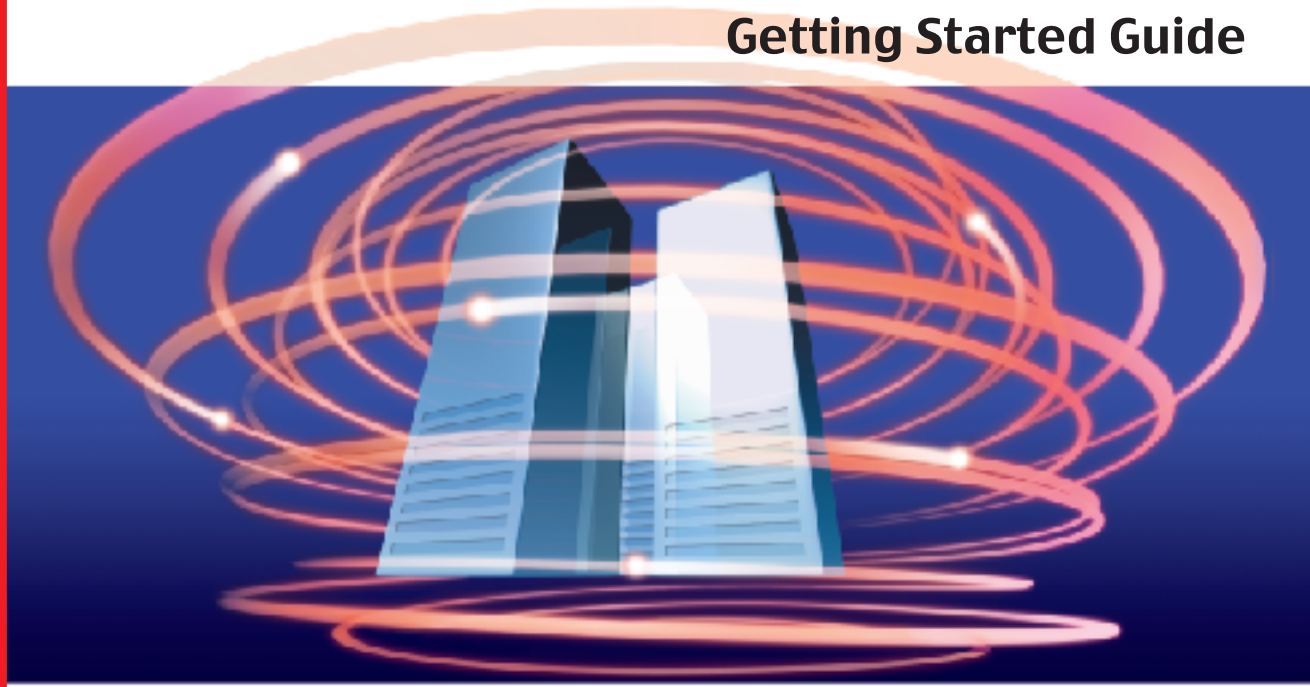
TREND MICRO™

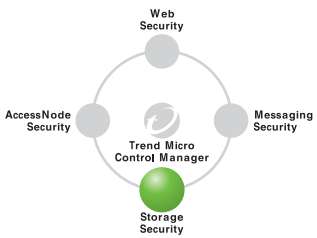
ServerProtect™ 1

Virus Protection for the Linux™ Platform

for Linux™

Getting Started Guide





TREND MICRO™

Item Code: SXEM1130921202
Release Date: December 2002
Protected by U.S. Patent No. 5,951,698

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

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

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at **docs@trendmicro.com**. Your feedback is always welcome. Please evaluate this documentation on the following site: www.trendmicro.com/download/documentation/rating.asp.

Contents

Chapter 1

Introducing ServerProtect for Linux

ServerProtect™ for Linux™ is the latest server-based antivirus solution from Trend Micro. It is a stand-alone, remote-manageable, antivirus system, specifically designed for Linux environments.

As a Trend Micro product, this application provides the added benefit of round-the-clock support that only Trend Micro's ISO-certified TrendLabs can provide.

This chapter discusses the following topics:

- Virus protection for Linux servers
- ServerProtect for Linux's features and capabilities
- How ServerProtect finds viruses
- System requirements

Virus protection on Linux servers

It is often mentioned that viruses are a non-issue for Linux-based computers. The operating system's built-in security features create an environment so hostile to viruses that the few Linux viruses that are created do not survive long enough to spread on any appreciable scale.

However, since work environments are often composed of a mix of Linux and non-Linux platforms -- the risk of Linux boxes becoming virus-havens, serving as launch pads for outbreaks within your network, remains a valid concern.

What's new with ServerProtect for Linux

The following features have been added in version 1.1:

Multiple-processor support

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

Manual and automated log deletion options

You can now delete logs on-demand, as well as according to a schedule.

Backup directory configuration

Relocate the backup directory to suit your needs.

Improved character set selection procedure for email notifications

Select the appropriate character set for your email notifications using a convenient drop-down menu.

What you can do with ServerProtect

ServerProtect has the following features:

Remote management via Web-browsers

ServerProtect for Linux is configured via a browser-based console. This allows you to control the application from any location. The console can be accessed via Microsoft Internet Explorer.

Real-time and scheduled scanning

In addition to on-demand scanning, or "Scan Now", ServerProtect can act against viruses automatically -- without user intervention. Real-time scanning checks files for viruses whenever they are accessed.

Scheduled scanning performs a thorough scan of your Linux machine at regular, user-specified, intervals. You can schedule these scans after office hours so as not to interfere with normal operations.

Manual or automated Internet-based updates

You can perform manual or scheduled updates of virus pattern, and scan engine files -- allowing you to retain the potency of your virus protection. Normally these updates are retrieved from Trend Micro's update servers; however the update source is configurable so you can set up your own update server on a local intranet server.

Notification of virus outbreaks

You, or anyone you designate, can receive email and/or Simple Network Management Protocol (SNMP) notifications about system or virus events, such as virus outbreaks, that occur on your ServerProtect machine. This allows you to always stay on top of developing virus situations, 24 hours a day, wherever you are.

Detailed and easy-to-maintain logs

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

How ServerProtect for Linux works

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

Pattern matching

ServerProtect draws upon an extensive database of virus patterns to identify viruses, and other malware, through a process called "pattern matching". Key areas of suspect files are examined for tell-tale strings of malware code and compared with thousands of virus signatures that Trend Micro has on record.

For polymorphic or mutation 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! You must keep your virus pattern file up-to-date. By some estimates, more than a thousand new viruses are created each year -- a rate of several a day.

MacroTrap

Macro viruses are application specific, and are not confined to a particular operating system. So long as an operating system supports the macro's application, it can be infected. Given this cross-platform compatibility, combined with the growing 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 is designed to provide you with a means of protecting your network from this malware-type.

How it works

The MacroTrap performs a rule-based examination of all macro code that is saved in association 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. Trend Micro's 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 (which are files composed of many, often compressed, files) are the preferred file formats for distribution via email or the Internet. Unless your antivirus application is specially equipped to handle these files, viruses and other malware may be "smuggled" into your network inside these files.

The ServerProtect scan engine can scan inside archives and compressed files. It can even detect viruses in compressed files and archives composed of other compressed files -- up to five compression layers deep.

The Trend Micro scan engine can detect malware in archives created by popular compression and archival algorithms, such as *.zip, *.arj, *.lzh. A more comprehensive list can be found on the online help.

Compressed File Scan Limit

As a system resource conservation measure, files within compressed archives that exceed a specific size are not scanned by ServerProtect. These files are skipped, and are recorded in the scan logs. Other files in the archive that do not exceed this limit are still scanned.

The skipped files can only be scanned if they are decompressed -- real-time scan can detect viruses in these files as they are extracted.

System requirements

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

Hardware

- An Intel™ Pentium II processor 266Mhz or higher.
- RAM 128MB or better
- 25MB of disk space for the /Opt directory
- 8MB of disk space for the /tmp directory

Software

Red Hat™ 7.2 - kernel 2.4.9-31

For other kernel and platform versions, go to the following URL:

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

and then click **Kernel Support** for additional information.

Web-based console compatible browsers

The ServerProtect Web-based console for this version can be accessed via Microsoft Internet Explorer 5.5 with Service Pack 2, or later.

Chapter 2

Installing ServerProtect for Linux

Here you will find step-by-step instructions for installing and uninstalling ServerProtect.

Installing ServerProtect

ServerProtect for Linux 1.1 is designed to operate with kernel 2.4.9-31. If the Linux server uses a different kernel, then you need to download a corresponding Kernel Hook Module from the Trend Micro Web site.

Note: You must be logged on as a root user when performing an installation.

To install on Linux servers with kernel version 2.4.9-31:

1. From the directory containing the ServerProtect Linux installation files, type the following at the command line:

   ```
   SProtectLinux-1.1.RedHat.i686.bin
   ```

   The above command extracts the required files in their proper places.

To install on Linux servers with kernels other than version 2.4.9-31:

1. Verify if your kernel is supported. Go to the following URL:

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

   and then click **Kernel Support**.

2. Click the operating system/platform that corresponds to your Linux server.

3. Click the Kernel Hook Module (KHM) package that corresponds to your kernel.

4. Click **Download now** to download the KHM package.

5. Install the latest version of ServerProtect, without starting the ServerProtect service. From the directory containing the ServerProtect installation files, type the following at the command line:

   `SProtectLinux-1.1.RedHat.i686.bin -f`

   The above command extracts the required files to their proper places.

6. Copy the KHM package to the following directory:

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

7. Go to the directory in step three, and then type the following command at the command line:

   `tar xzvf {kernel version}.tgz`

   The following files are extracted from the package:

   - {kernel version}.md5
   - splxmod-{kernel version}.o
   - splxmod-{kernel version}smp.o

8. Start the ServerProtect service. Type the following at the command line:

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

About KHM versions

KHMs are named after their corresponding kernels. For example, the KHM for kernel 2.4.18-10 is 2.4.18-10.tgz.

Removing ServerProtect

Before removing ServerProtect, you must log on as a root user. At the prompt, enter the following:

```
rpm -e SProtectLinux
```

The above command will automatically stop the ServerProtect service and remove the application.

Upgrading ServerProtect

Users of older version of ServerProtect for Linux must manually remove their existing software before installing version 1.1.

WARNING! *Before removing your existing version of ServerProtect, verify if your kernel has a corresponding Kernel Hook Module.*

Converting ServerProtect trial version

Whenever you install ServerProtect, you are actually installing a 30-day trial version of the product. To continue using this product after the trial period, you must register it.

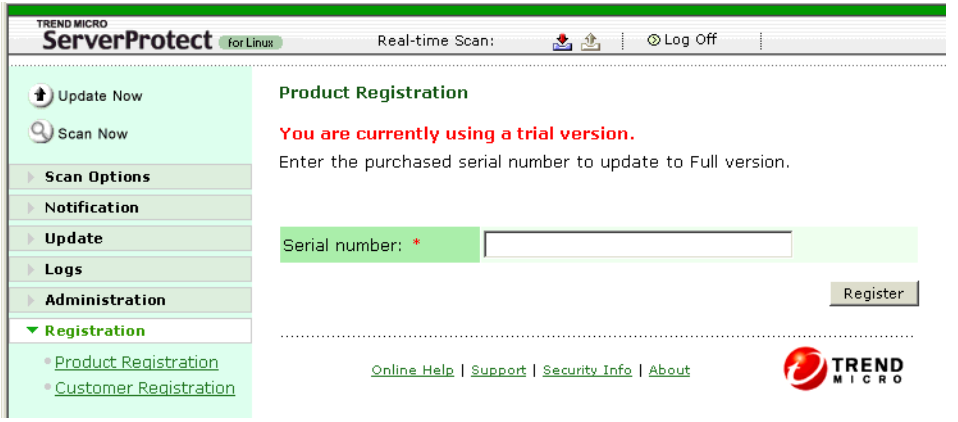


FIGURE 2-1. Product registration page

Use the serial number included in the ServerProtect package, or purchase one from your Trend Micro reseller, then either register from the logon or Product Registration screens.

To register from at the logon screen:

Type the serial number in the **Serial Number** field on the logon screen, and then click **Register**.

Register from the Product Registration screen:

1. Select **Registration** > **Product Registration** from the left-hand menu.
2. Enter the serial number in the **Serial Number** field, then click **Register**.

Customer registration

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance.

To register your software:

1. Click **Registration** > **Customer Registration**. The online registration page of the Trend Micro Web site opens.
2. Provide the following required registration information on the page:
   - Product name - choose a product from the drop-down menu
   - Version #
   - Language - select a language from the drop-down menu
   - Serial #
   - First Name
   - Last Name
   - Email Address
   - Country
   - Telephone

   Enter the optional information, those without the asterisk (*), when applicable.
3. Click **Submit**.

Chapter 3

Getting Started with ServerProtect

This chapter helps you to start using ServerProtect; it provides basic setup and usage instructions. Additional information is available in the online help.

The following topics are covered here.

- Starting and Stopping ServerProtect
- The ServerProtect Web Console
- Updating your Scan Engine and Virus Pattern
- Configuring and Performing Scans
- Configuring Notifications

Starting and stopping ServerProtect

ServerProtect must be started from either the command line, or the Linuxconf utility.

Note: By default, ServerProtect starts whenever the server it is installed upon is turned on. It is, however, possible to change this setting. For details *see Configuring start-up settings* on page 3-3.

Starting ServerProtect

There are two ways to start ServerProtect: from the command line, or from the Linuxconf utility.

Note: You must be logged on as a root user to start ServerProtect for Linux.

To start ServerProtect from the command line:

1. Log on as a root user.
2. Type the following at the command line:

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

   The message "ServerProtect for Linux is running" appears.

To start ServerProtect from the Linuxconf utility:

1. Log on as a root user.
2. Go to **Control** > **Control Panel** > **Control Service Activity**.
3. Scroll down to SPLX, then press ENTER. The Service SPLX screen opens.
4. Select **Start**.

Stopping ServerProtect

There are two ways to stop ServerProtect:

- From the command line
- From the Linuxconf utility

Note: You must be logged on as a root user to stop ServerProtect for Linux.

To stop ServerProtect from the command line:

Type the following:

```
/etc/rc.d/init.d/splx stop
```

To stop ServerProtect from the Linuxconf utility:

1. Go to **Control** > **Control Panel** > **Control Service Activity**.
2. Scroll down to SPLX, then press Enter. The Service SPLX screen opens.
3. Select **Stop**.

Configuring start-up settings

By default, ServerProtect for Linux starts automatically when the server is turned on. You can, however, change this setting using the Linuxconf utility.

To configure start-up settings:

1. Log on as the root user, then run the Linuxconf utility from the command line. The utility's UI appears.
2. Go to **Control** > **Control Panel** > **Control Service Activity**. The Service Control window appears.
3. Select **SPLX** to open its service window.
4. Toggle the **Automatic** check box with the space bar to set SPLX to start either automatically or manually.

The ServerProtect Web console

ServerProtect is controlled via a Web-based console -- it is the only way to access its features. The console permits remote, multiple-user control of the application via Microsoft Internet Explorer. It provides a feature-rich interface that allows you to manage ServerProtect from virtually any location with an Internet connection.

To access the console:

1. Type the location of the ServerProtect host and the static port used for the console in the browser's address field. For example:

   `http://{host name}:14942/`

   Where:

   {host name} - is either the computer's host name or its IP address

   14942 - is the default port number used by ServerProtect

Note: If you need to change the above port number, use the *splxport* tool; see *splxport* on page A-3.

2. Type your logon password, then click **Enter**. The default password is blank.

To log off from the console:

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

Things to remember about the console

- The Web console provides access to all ServerProtect functions. However it cannot start or stop the application. This must be accomplished either from the command line or the Linuxconf utility; see *Starting and stopping ServerProtect* on page 3-1.
- The console is automatically refreshed every hour. You can, however, refresh it manually as often as you require.
- The console can be used by more than one individual -- simultaneously. In the event of conflicting commands, ServerProtect performs the last instruction applied or saved. There is currently no way for two users to monitor the other's commands.

To configure passwords:

1. Select **Administration** > **Password** from the left-hand menu.
2. Type the current password in the appropriate field.
3. Provide a new password. Passwords must not be longer than 32 characters, and can only contain alphanumeric characters and hyphens ('-').
4. Re-type the password for confirmation.
5. Click **Save**.

Note: Always protect your Web console password. Trend Micro recommends that you set your password immediately after installation. There is no default password.

Updating your scan engine and virus pattern

Since new viruses are created daily, the engine and pattern files that came with your copy of ServerProtect might no longer be able to protect you against the latest threats. After installing ServerProtect, Trend Micro highly recommends updating the following files using ServerProtect's Internet-based component update feature:

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

Updates can be performed either manually, or according to a schedule. Trend Micro recommends performing a manual update immediately after installation. Only registered users are eligible for scan engine and virus pattern updates; see *Customer registration* on page 2-4.

Note: Since updates are obtained through the Internet, make sure ServerProtect's proxy settings have been configured before attempting an update.

To configure proxy settings:

1. Select **Update** > **Proxy Settings** from the left-hand menu.
2. Select the **Use a proxy server to access the Internet** check box.
3. Provide the following information as required:
   - **Proxy server** - specify either the proxy server's IP address or name
   - **Port** - type the port the proxy uses

   If your proxy requires authentication, supply the following:

   - **User ID**
   - **Password**

Configuring a manual update

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

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

To use the saved settings:

Click Update Now on the left-hand menu.

To update after configuring update settings:

1. Select **Update** > **Manual Update** on the left-hand menu. The Manual Update screen appears.
2. Select the check box of the component you want to update. The latest available version of the component is shown to the right of the component label.

	Component	Current Version
☑	Virus Pattern	333
☑	Scan Engine	6.27

FIGURE 3-1. Components to update

3. Select a download source.

FIGURE 3-2. Download source

There are two options:

- **Trend Micro update server**

- **Other Internet source** - to use this option you must place the update components on a Web server. Provide the host name or IP address, and directory (for example, www.download.com/download).

4. Click **Save & Update**.

Configuring a scheduled update

Scheduled Updates allow you to perform regular updates automatically -- thereby reducing your workload.

To configure a scheduled update:

1. Select **Update** > **Scheduled Update** on the left-hand 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 options are:
   - Virus pattern
   - Scan engine
4. Configure a download schedule. Select a Start time in hours and minutes from the **Start time** menu.

FIGURE 3-3. Download schedule

5. Specify a repeat interval. The options are **Hourly**, **Daily**, and **Weekly**. For weekly schedules, specify the day of the week (for example, Sunday, Monday, and so on.)
6. Select a download source. There are two options:
   - **Trend Micro update server**

- **Other Internet source** - to use this option you must place the update components on a Web server. Provide the host name or IP address, and directory (for example, www.download.com/download).

Configuring and performing scans

Once ServerProtect is installed, and the virus pattern and scan engine have been updated, you can configure the scanning options.

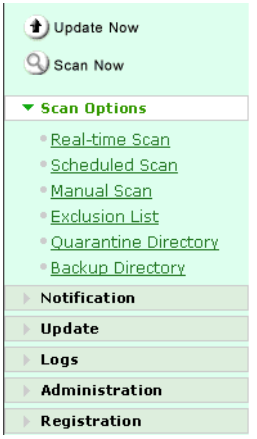


FIGURE 3-4. Left-hand menu; Scan Options

ServerProtect can perform three types of scanning: Real-time, Manual (Scan Now), and Scheduled Scan. These are explained below:

Scan Type	Description
Real-time	This type of scan runs each time a file is accessed or executed. It can scan both incoming and outgoing files.
Manual	Also known as Scan Now, this performs a thorough scan of your server -- on demand.
Scheduled	This is similar to a Manual Scan, except that it is performed according to a specified schedule.

Table 3-1. Types of Scanning

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

Note: The scanning technologies employed are explained in Chapter 1; see *How ServerProtect for Linux works* on page 1-4.

Understanding virus actions

A variety of actions can be performed on detected viruses -- all of which can be peformed by the scan types mentioned above. These are shown below.

Action	Description
Pass	Record virus infections or malicious files in the scan logs, but take no action.
Delete	Remove infected or malicious files.
Rename	Modify the infected file's extension to prevent it from being opened or executed. Renamed files are given the extension "VIR".
Quarantine	Move infected or malicious files to a restricted access folder.
Clean	Removes virus code from infected files.

Table 3-2. Virus Action

To specify locations to scan:

1. On the left-hand menu, select **Scan Options**, then choose the scan method you want to configure.
2. Under the Directories to Scan section, select the desired scan coverage

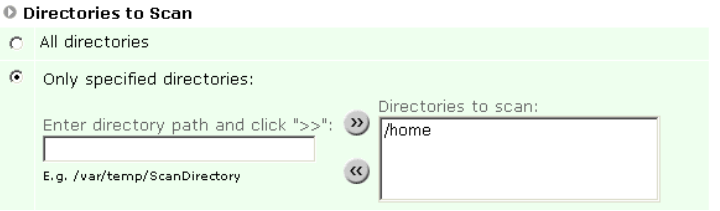


FIGURE 3-5. Directories to scan

The options are:

- **All directories** - scans all directories, except those included in the Exclusion List. For additional information on the Exclusion List, refer to the online help at Using ServerProtect for Linux > Configuring Exclusions Lists > What is the Exclusion List?
- **Only specified directories** - limits the scan to the directories that you specify. To do so, do the following:

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

  b. Click » to add the entry to the Directories to Scan list.

  c. Add other directories as required.

To remove directories that were previously specified:

a. Select the directory for removal in the Directories to Scan list. To select consecutive directories, click the first item, press and hold down Shift, and then click the last directory. For non-consecutive directories, press and hold down Ctrl and then click each directory.

b. Click « to remove the selected entry.

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

Specifying files to scan

ServerProtect can be configured to scan only files that are known to be vulnerable to infection. This significantly reduces scanning time, and is an effective system resource conservation measure. Each scan type can be configured separately.

To specify files to scan:

1. On the left-hand menu, select **Scan Options**, then choose the scan method you want to configure.
2. Under File Types to scan, click the desired scan coverage.

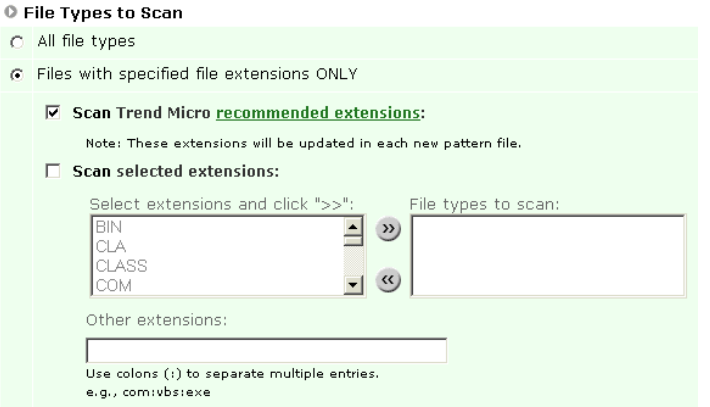


FIGURE 3-6. File types to scan

The options are:

- **All files types** - Scans all files, except for those specified in the Exclusion List. For additional information on the Exclusion List, refer to the online help at Using ServerProtect for Linux > Configuring Exclusions Lists > What is the Exclusion List?
- **Files with specified extensions ONLY** - Restricts scanning to selected file extensions. This option also has three sub-options, which can be enabled either individually or in combination. These are:

- **Scan Trend Micro recommended extensions** - This option takes advantage of the constantly updated extensions list embedded within the virus pattern.
- **Scan selected extensions** - You can specify extensions from a list of extensions. To do so, do the following:

  a. Select the extension from the left-hand list. To select consecutive extensions, click the first item, press and hold down SHIFT, and then click the last extension. For non-consecutive extensions, press and hold down CTRL, and then click each item

  b. Click  to add the extension to the File Types to Scan list.

  To remove previously excluded extensions:

  a. Select the extension from the right-hand list. See the previous step for multiple selection instructions.

  b. Click  to remove the extension from the File Types to Scan list.

- **Other extensions** - Type custom file extensions in this textbox. Use semicolons (;) to separate entries. For example:

  ```
  LGL;FIN;ADM
  ```

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

Scanning compressed files

ServerProtect scanning options can be independently configured to handle compressed files and archives -- a useful option considering compressed file scanning is a resource-intensive process.

To scan compressed files:

1. On the left-hand menu, select **Scan Options**, then choose the scan method you want to configure.
2. Under the Compressed File section, select the **Scan compressed files** check box.

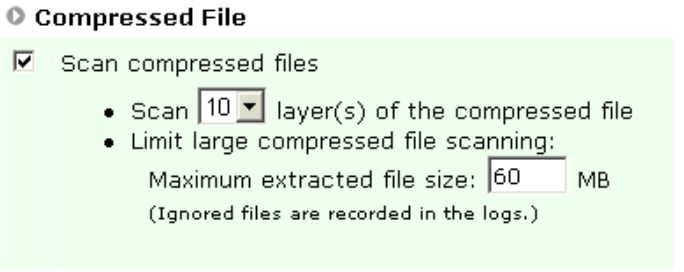


FIGURE 3-7. Compressed file scanning

3. Specify the number of scanning layers to be scanned. The permitted values are from 1 to 20 layers. The default settings are 5 layers for Manual and Scheduled scanning, and 1 layer for Real-time scanning.
4. Specify the maximum file size that will be extracted 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 30MB for Real-time and Scheduled scanning.
5. Click **Save** to apply your settings.

Configuring Real-time Scanning

When enabled, Real-time scan runs in the background; constantly checking all accessed files.

Enabling Real-time Scan

Trend Micro recommends that you keep Real-time scanning enabled at all times.

To enable Real-time Scan:

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

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

Real-time Scan options

Real-time scan has the following scanning options:

- **Directories to Scan**. Choose to scan only specific directories; see *To specify locations to scan:* on page 3-10
- **File Types to Scan**. Choose to scan specific file types; see *To specify files to scan:* on page 3-12
- **Action When Viruses are Found**. Click the appropriate action (clean, quarantine, rename, delete, or pass) to be taken when a virus, or other malware, is detected; see *Understanding virus actions* on page 3-10 for details of each action.
  While configuring virus actions, decide whether or not to save a backup copy of files that are cleaned. On rare occasions, the scan engine may damage the files it cleans.

  To make a backup, select the **Back up files to a specified folder before cleaning** check box.
- **Compressed File**. Real-time scanning can be performed on compressed files and archives; see *To scan compressed files:* on page 3-13.

Setting scan direction

Real-time scan can detect viruses in both incoming and outgoing files. Incoming files are those that are being placed on your server, whereas outgoing files are copied or moved from your server to another location.

View the Real-time Scan icon on the title bar to verify the status of the scan direction.

FIGURE 3-8. Title bar showing Real-time scan with inbound scanning enabled

The icons are shown below:

Scan Direction	On	Off
Incoming		
Outgoing		

Table 3-3. Scan Direction Icons

To specify the scanning direction for Real-time scan:

1. Select the **Incoming** or **Outgoing** check boxes, to activate scanning for the desired direction.
2. Click **Save** to apply your settings.

Configuring a Manual Scan (Scan Now)

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

To use the saved settings:

Click 

on the left-hand menu.

To scan after configuring scan settings:

1. Select **Scan Options** > **Manual Scan** on the left-hand menu. The Manual Scan screen appears.
2. Configure the scan settings as required; see *Manual Scan options* on page 3-18.
3. Click **Scan Now**. The following confirmation window appears.

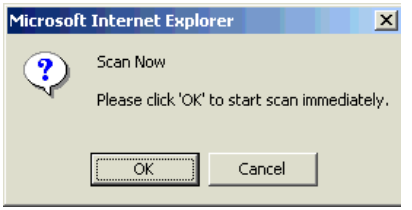


FIGURE 3-9. Scan Now confirmation window

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

After the scan is performed, the scan progress window showing the status of the scan appears.

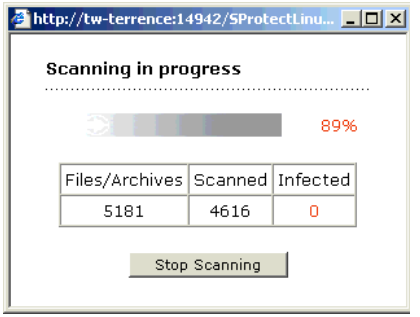


FIGURE 3-10. Scan progress window

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

To stop a Manual Scan:

Click **Stop Scanning** on the scan progress screen.

Manual Scan options

Manual scan has four options that can be configured. These can be accessed by clicking **Scan Options** > **Manual Scan** on the left-hand menu.

- **Directories to Scan**. ServerProtect can be made to restrict scanning to specific directories. see *To specify locations to scan:* on page 3-10
- **File Types to Scan**. You can limit scanning to specific file types. see *To specify files to scan:* on page 3-12
- **Action When Viruses are Found**. Click the appropriate action (clean, quarantine, rename, delete, or pass) to be taken when a virus, or other malware, is detected; see *Understanding virus actions* on page 3-10 for details about each action.
  While configuring virus actions, decide whether or not to save a backup copy of files that are cleaned. On rare occasions, the scan engine may damage the files it cleans.

To make a backup copy, select the **Back up files to a specified folder before cleaning** check box.

- **Compressed File**. Manual scanning can be performed on compressed files and archives; see *To scan compressed files:* on page 3-13.

Configuring a Scheduled Scan

Scheduled scanning is similar to Manual scanning, except that it is activated automatically -- according to the schedule that you specify.

Enabling Scheduled Scanning

Trend Micro recommends enabling Scheduled Scanning to make sure that your servers are free of viruses.

To enable Scheduled Scan:

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

Scheduled Scan options

Scheduled scan has the following scanning options:

- **Directories to Scan**. ServerProtect can be made to restrict scanning to specific directories; see *To specify locations to scan:* on page 3-10
- **File Types to Scan**. You can limit scanning to specific file types; *see To specify files to scan: on page 3-12*
- **Action When Viruses are Found**. Select the appropriate action (clean, quarantine, rename, delete, or pass) to be taken when a virus, or other malware, is detected; see *Understanding virus actions* on page 3-10 for details about each action.
  While configuring virus actions, decide whether or not to save a backup copy of files that are cleaned. On rare occasions, the scan engine may damage the files it cleans.

  To make a backup copy, select the **Back up files to a specified folder before cleaning** check box.

- **Compressed File**. Scheduled scanning can be performed on compressed files and archives; see *To scan compressed files:* on page 3-13.

Scan frequency

You can schedule how often ServerProtect scans your computer.

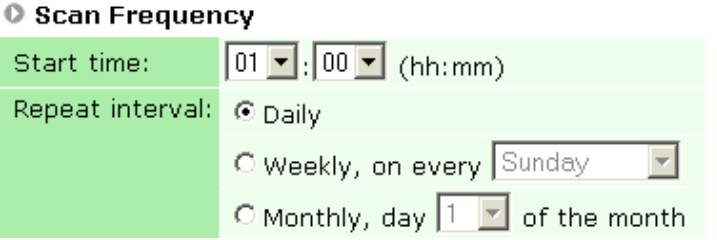


FIGURE 3-11. Scan Frequency

To specify the scan frequency:

Provide the following information:

Start time - This refers to the specific hour that the scan starts.

Repeat interval - Specify how often you want the scan to be performed.

Viewing scan results

There are two ways to view scan results:

- Using the Scan Now complete screen (for Manual Scan only)
- Using the Scan and Virus logs

Using the Scan Now complete window

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

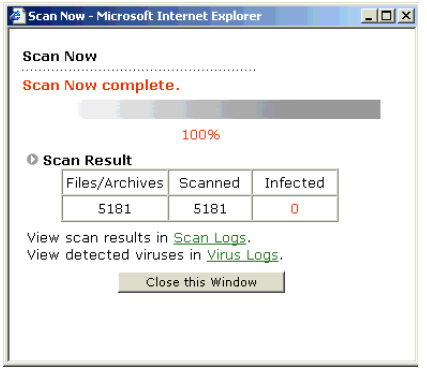


FIGURE 3-12. Scan Now complete window

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

Using scan and virus logs

Scan Logs record information about scans performed or attempted. Virus logs, on the other hand, keep track of viruses that were encountered and the measures taken against them.

To view these logs:

1. Select **Logs** from the left-hand menu, and select the kind of log that you want to view.

Note: For information about other types of logs, and log maintenance, refer to the online help.

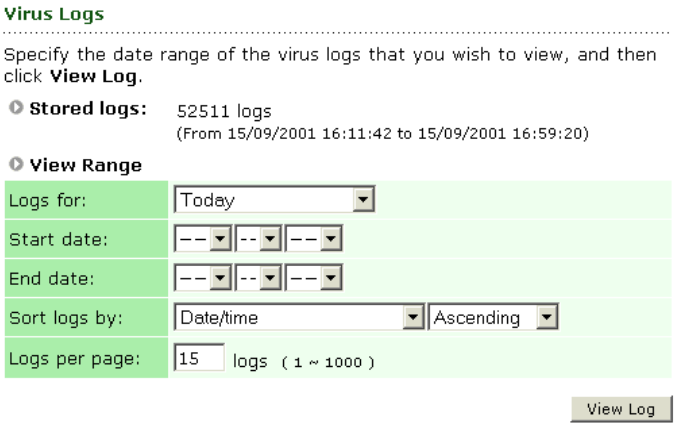


FIGURE 3-13. Virus logs

2. Specify the query criteria for the logs that you want to view. The parameters are:
   - **Logs for** - Select among the commonly specified date ranges: **All dates**, **Today**, **Yesterday**, **Past 7 days** or **Past 30 days**. If the period you require is not covered by the above options, choose **Specified date range** -- this enables the Start and End date fields.
   - **Start date** - Type the earliest log you want to view. Select the **Specified date range** option in **Logs for** to use this criteria. The month-day-year format is used.
   - **End date** - Type the latest log you want to view. Select the **Specified date range** option in **Logs for** to use this criteria. The month-day-year format is used.
   - **Sort logs by** - Specify the order and grouping of the logs. Options for groups are: **Date/time**, **Scan type**, and **Status**; the order may either be ascending or descending.
   - **Logs per page** - Select the number of logs to be displayed at a time; choose a setting that is appropriate for your monitor resolution. The permitted values are from 1 to 1,000 logs.
3. Click **View Log** to begin the query.

Specifying the Quarantine Directory location

Occasionally, the scan engine will not be able to clean certain files. If you do not want to delete these files, the only recommended alternative is to move the file to the ServerProtect Quarantine Directory. The default location is:

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

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

To specify a Quarantine Directory:

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

Note: If you change the location of this directory, existing files will still remain in the original location. Only newly quarantined files will be placed in the new directory.

Specifying the Backup Directory location

You can change the default backup directory at the Backup Directory screen. The default location is:

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

To specify a Backup Directory:

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

Note: If you change the location of this directory, existing files will still remain in the original location. Only newly backed-up files will be placed in the new directory.

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. Notifications can be sent to several individuals at once.

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

Setting alert events

You can specify the events that require alerts, as well as the messages that are sent. This section provides instructions on how to:

- Change alert settings
- Select alert events
- View default messages
- Make custom messages

To change alert settings:

1. Select **Notification** > **Alert Settings** from the left-hand menu. The Alert Settings screen appears.
2. Click **Alert Settings**.
3. Select the check boxes of the alerts that you want to send:
   - **Enable outbreak alert** - This sends out a warning 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.
   - **Enable standard virus infection notification** - This sends out a notification each time a virus is detected on your system. One notification will be sent out for each detected virus.
   - **Enable Real-time scan configuration change notification** - Alerts are sent whenever Real-time Scan settings are modified.
   - **Enable ServerProtect On / Off notification** - Notifications are sent whenever the ServerProtect service is started or stopped.

- **Enable virus pattern out-of-date notification** - This warns you if your virus pattern file is a specific number of days old. You can define the age parameter on this page.

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

To view default messages:

On the Alert Settings screen, click **default messages**. This shows a read-only list of default messages.

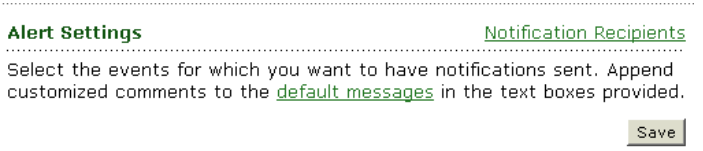


FIGURE 3-14. Default message link

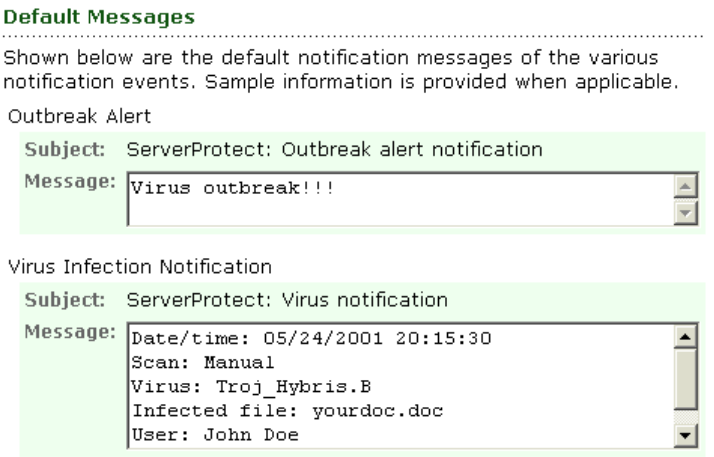


FIGURE 3-15. Selected default messages

To make custom messages:

You can append your own custom message to the different notifications. Type your message in the boxes labelled "message" under the different alert events.

Notification recipients

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

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

To enable SMTP mail notification:

1. Select the **Enable SMTP Mail Notification** check box.
2. In the **Server name** text box, type either the SMTP server name or its IP address, for example:

   `smtp.server.com` or 210.192.229.11
3. Specify the port to be used in the **Port** field.
4. Type your email address in the **From** field.

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

---

5. Specify the recipient's addresses. To add an address do the following:

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

   `yourname@yourCompany.com`

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

   To remove an address from the list:

   a. Select an address from the recipients list. To select consecutive addresses, click the first item, press and hold down Shift, and then click the last address. For non-consecutive addresses, press and hold down Ctrl, and then click each item.

b. Click  to remove the selected entry from the recipients list.

6. Specify a character set to use in the **Character set** field; the default is the Western European character set: iso-8859-1. There are two ways to do this:
   - Type the character set code in the **Character Set** field. For information on other commonly used character sets, see *SMTP mail notification character sets* on page A-4.
   - Click **Options**, and then choose the appropriate character set.
7. Click **Save** to apply the changes.

To modify recipient settings:

1. Do either of the following to access recipient settings:
   - Select **Notification** > **Recipients** on the left-hand menu
   - Click **Recipients** on the Alert Settings screen
2. Make the appropriate modifications, then click Save.

To enable SNMP notification:

1. Select the **Enable 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** to apply the changes.

Chapter 4

Troubleshooting and Contacting Technical Support

This chapter provides the following information:

- Troubleshooting tips for selected ServerProtect problems
- Technical support information

Troubleshooting

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

Default password

ServerProtect for Linux does not have a default password. You are therefore strongly advised to set one immediately after installation.

Web console rejects all passwords

This situation may be caused by a number of factors:

- **Incorrect password**. Passwords are case sensitive, for example 'TREND' is different from 'Trend', or 'trend'.

- **ServerProtect has not been started**. ServerProtect can be configured not to start automatically when the server is turned on. To start ServerProtect, type the following at the prompt:

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

- **Your 30-day trial period has expired**. You will be automatically locked out of your management console after 30 days if you do not register your product. If this happens, obtain a serial number for your product, then type it in the **serial number** field at the logon screen.

Testing your installation

The European Institute of Computer Antivirus Research (EICAR), in cooperation with antivirus vendors, has developed a test file that can be used to check if your system can, in fact, detect viruses.

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

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

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

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

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

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

Contacting technical support

A license to Trend Micro antivirus software includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

Evaluation copies of all Trend Micro products can be downloaded from Web site, www.trendmicro.com.

Trend Micro Incorporated

10101 N. De Anza Blvd.

Cupertino, CA 95014- 9985

Tel: +1 (408) 257-1500, +1 (800) 228-5651

Fax: +1 (408) 257-2003

Online resources

Email: sales@trendmicro.com

Web: www.trendmicro.com

Knowledge Base: solutionbank.trendmicro.com/solutions/solutionSearch.asp

Security Information: www.trendmicro.com/vinfo

Security information

Comprehensive security information is available at the Trend Micro Web site:

```
www.trendmicro.com/vinfo/
```

Use the Web site to learn about:

- Computer virus hoaxes
- A weekly virus alert, listing the viruses that will trigger during the current week
- How to determine if a virus detection is a false alarm

- Trend Micro Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- A basic guide to computer viruses
- Trend Micro virus reading room, with dozens of articles about the latest issues in computer viruses, including the threat posed by Java applets and ActiveX controls
- Product details and white papers

Knowledge Base

Trend Micro provides Knowlege Base, an online database filled with answers to technical product questions. Use it, for example, if you are getting an error message and want to find out what to do to. Type the following URL in your browser's address bar:

solutionbank.trendmicro.com/solutions/solutionSearch.asp

New solutions are added daily. However, if you don't find the answer you seek, you can submit your question online, where a TrendLabs engineer will provide you with an answer or contact you for more information.

TrendLabs™

TrendLabs 24x7 global antivirus research and support centers form the backbone of the Trend Micro service infrastructure. A team of more than 250 engineers operates around the clock at sites spanning the globe to keep customers informed and protected against the latest security threats. TrendLabs includes service centers in Tokyo, Paris, California, Taipei, Munich and its ISO 9002-certified headquarters in Metro Manila.

Sending your infected files to Trend Micro

You can send your viruses to Trend Micro via email. More specifically, if you have a file that you think is infected with a virus but our scan engine does not detect it or cannot clean it, we encourage you to send the suspect file to us at the following address:

```
virus_doctor@trendmicro.com
```

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

Appendix

This chapter provides additional information about ServerProtect tools, and miscellaneous product information.

SPLX script

ServerProtect can be started and stopped using the SPLX script. The script's parameters are:

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: Displays currently active ServerProtect threads

Apache configuration file

ServerProtect uses its own Apache server. Its configuration file can be found on the following path:

```
/opt/TrendMicro/SProtectLinux/SPLX.httpd/conf/splxhttpd.conf
```

Log files

Log files are kept in the following directory:

```
/opt/TrendMicro/SProtectLinux/SPLX.httpd/log
```

ServerProtect tools

The ServerProtect package comes with three tools that are designed to address certain customization issues. The tools can be found in the following directory:

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

These are explained below:

splxcomp

This tool is designed to address compatibility issues between Trend Micro InterScan™ VirusWall™ for Linux and ServerProtect. This tool must be run when both applications are installed on the same machine.

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

splxpasswd

This tool resets the Web console password to blank. The tool can only be used by a user with super user privileges.

Syntax:

```
splxpasswd {-h} {-v} {-r}
```

Parameters:

-h: Displays the tool's parameters list

-v: Displays version information

-r: Resets the ServerProtect Web console. The resulting password is blank.

splxport

This changes the port that ServerProtect uses.

Syntax:

```
splxport {-h} {-v}{-p port_number}
```

Parameters:

-h: Displays the tool's parameters list

-v: Displays version information

-p: Resets the port used by ServerProtect for Linux

SMTP mail notification character sets

The following is a sampling of the character sets that can be used with ServerProtect. For information on how these character sets are used; see *To enable SMTP mail notification:* on page 3-26.

Character Set	What you should type in the Charset field
English	us-ascii
Korean	euc-kr
Latin 1 Western European (default)	iso-8859-1
Japanese	iso-2022-jp
Traditional Chinese	big5
Simplified Chinese	gb2312

Table A-1. Common Character Sets

Index

S

T