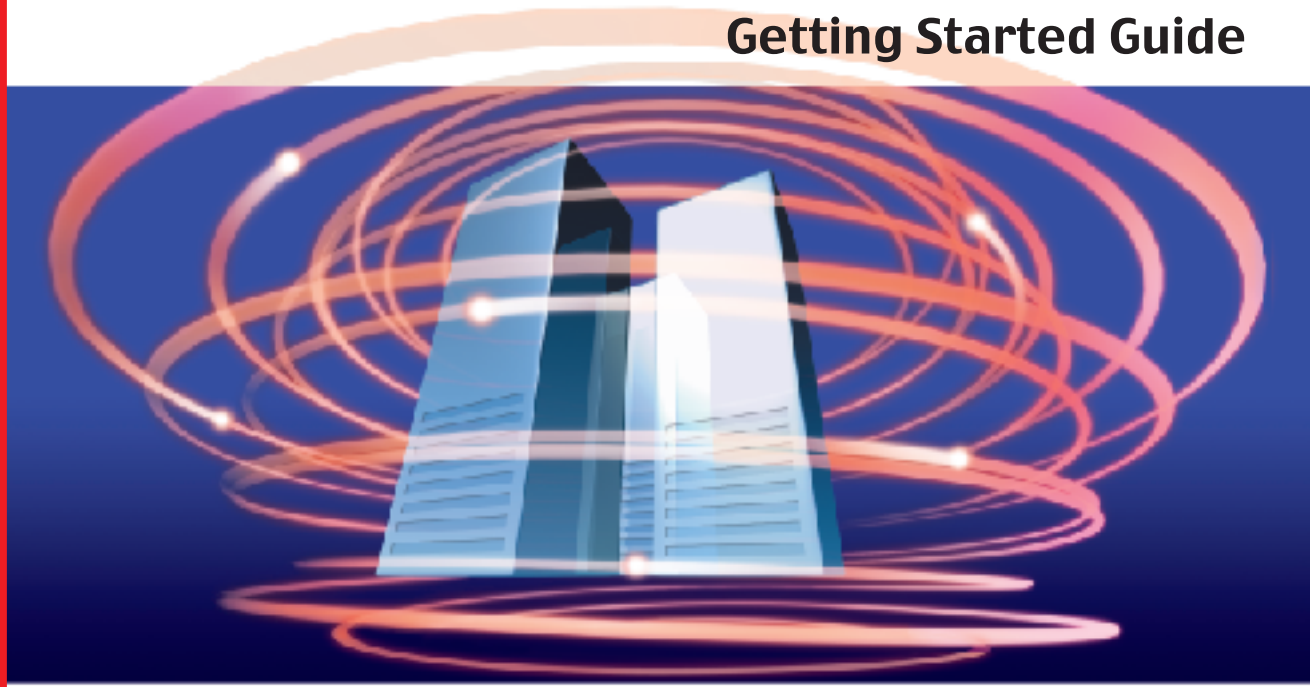
TREND MICRO™

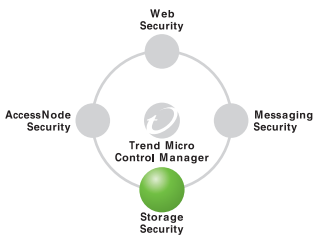
ServerProtect™ 1

Virus Protection for the Linux™ Platform

for Linux™

Getting Started Guide





TREND MICRO™

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

`www.trendmicro.com/download`

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be reviewed on an annual basis at Trend Micro's then-current Maintenance fees.

Document Part No. SPEM11792/40318

Release Date: June 2004

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

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

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

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

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

Contents

Chapter 1

Introducing ServerProtect™ for Linux™

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

This chapter discusses the following topics:

ServerProtect for Linux Features and Capabilities

ServerProtect has the following features:

Multiple-processor support

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

Manual and automated log deletion options

Delete logs on-demand and according to a schedule.

Backup directory configuration

ServerProtect can back up infected files before Real-time Scan, Scan Now, or scheduled scan performs the Clean action. This is useful when an infected file cannot be cleaned and as a result, it is not recoverable. As a precaution, you may wish to create backup copies of your files.

Improved character set selection procedure for email notifications

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

Remote management via Web-browsers

You can configure ServerProtect for Linux via a browser-based console (Microsoft™ Internet Explorer and Mozilla).

Real-time and scheduled scanning

In addition to manual scanning, or "Scan Now", ServerProtect can act against viruses without user intervention (Scheduled Scan). ServerProtect can also check files for viruses in real-time (Real-time Scan).

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.

Manual or automated Internet-based updates

To retain virus protection potency, you can perform manual or scheduled updates of virus pattern and scan engine files. Normally you retrieve these updates 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. To set up your own update server, contact technical support.

Notification of virus outbreaks

Users can receive email and/or Simple Network Management Protocol (SNMP) notifications about system or virus events, such as virus outbreaks, that occur on a ServerProtect machine.

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 according to a custom schedule, to keep them from becoming too large.

What's new in ServerProtect for Linux

The following new features are available in version 1.3:

Kernel dependent and independent modes

ServerProtect 1.3 comes in two modes:

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

  KHM installation is no longer a separate process– ServerProtect automatically installs the appropriate KHM for supported Linux distributions and kernels. The Real-time Scan page is the default page for the ServerProtect for Linux Web console in kernel-dependent mode.
- Kernel-independent mode– ServerProtect provides manual and scheduled scanning for Linux distributions and kernels that do not support the Kernel Hooking Module embedded in the installation program

  All real-time scan related options in the ServerProtect Web console are disabled. In addition, the Manual Scan page is the default page for the ServerProtect for Linux Web console in kernel-independent mode.

Support for advanced ActiveUpdate options

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

Component update now provides the following options:

- Digital signature checking– by default, ServerProtect implements this feature 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

The following proxy server types and authentication methods are supported in this version:

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

Consistency checking between ServerProtect Web console and configuration file (`tmsplx.xml`)

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

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

Support for new virus pattern file numbering format

ServerProtect 1.3 uses a new pattern file numbering format: n.nnn.nn. Under this system, the first 4 digits represent the pattern file number and the last two digits represent the file's build or controlled release version.

Support for Intel™ Hyper-Threading Technology

ServerProtect can be installed on servers running Intel's Hyper-Threading Technology. Please refer to the Intel Website for more details on Hyper-Threading Technology.

Support for Trend Micro Online Registration system

Use your Registration Key to register ServerProtect and obtain an Activation Code (formerly known as serial number) on the Trend Micro Registration Website.

New debug options for detailed debugging

ServerProtect 1.3 provides the following debug options:

- Kernel debugging– debugs kernel-related actions
- User debugging– debugs user-related actions

See *Debugging ServerProtect* on page 4-3 for details.

Virus Protection on Linux Servers

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

Linux system administrators can use both a Web-based console and the command line to manage virus outbreaks, virus scanning, virus pattern file updates, and notifications.

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". 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 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! *Due to the large number of new viruses, the virus pattern file should remain up-to-date.*

MacroTrap

Macro viruses are application specific; this means they can attack multiple operating systems. 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 provides 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 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. 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 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 twenty (20) 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 is available under *How ServerProtect Finds Viruses* in the online help.

Compressed File Scan Limit

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

Real-time Scan will still detect viruses included in skipped files during a decompression attempt.

Chapter 2

Installing ServerProtect for Linux

Here you will find instructions for installing and removing ServerProtect.

This chapter discusses the following topics:

System Requirements

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

Hardware

- Intel™ Pentium™ II processor (or higher) or AMD™ Athlon™ processor
- 128MB RAM or more
- 25MB of available disk space for the `/opt` directory
- 8MB of available disk space for the `/tmp` directory

Supported distributions and kernels

- Red Hat Enterprise Linux (AS, ES, WS) 2.1

  Note: ServerProtect in kernel-independent mode is the mode supported for these distributions. Therefore, only manual and scheduled scanning is available.

- Red Hat Enterprise Linux (AS, ES, WS) 3.0
  - 2.4.21-4.EL smp
  - 2.4.21-4.EL up
  - 2.4.21-9.0.1.EL smp
  - 2.4.21-9.0.1.EL up

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

Supported Web browsers for ServerProtect Web console

Access ServerProtect 1.3 Web console through the following browsers:

- Microsoft™ Internet Explorer 5.5 with Service Pack 2 or higher
- Mozilla 1.4 or higher

Note: Install Sun Micro™ Java™ 2 Runtime Environment 1.4.2_01 when using Mozilla to access ServerProtect Web console. Otherwise, product registration and access to the ServerProtect online help will not work.

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

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

Note: The `libgcc-3.2.2-5.i586.rpm` (or above) package should be installed. Otherwise, accessing the ServerProtect Web console via a Mozilla browser will not work.

Supported XWindow graphical desktop environments for simple GUI console

KDE 2.2.2-2 or higher

Note: The Quick Access console is provided only when you are logged on as root.

Registering ServerProtect

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. Register ServerProtect to ensure eligibility to receive the latest security updates and other product and maintenance services.

Note: Purchase a Registration Key from a Trend Micro reseller to obtain an Registration Key.

To register your software:

- If you have a serial number (that is, a ServerProtect 1.2x serial number)
  - **a.** Click **Registration** > **Customer Registration** from the left-hand menu. The Online Registration page of the Trend Micro Web site opens.
  - **b.** Fill out the online registration form, and then click **Submit**.

  Note: The serial number that comes with ServerProtect 1.2x can be used to register and activate ServerProtect 1.3.

- If you have a Registration Key (purchased from a Trend Micro reseller)
  - **a.** Using a Web browser, go to `https://olr.trendmicro.com/registration`.
  - **b.** Under **New customer registration**, click **Register Your Product**.
  - **c.** On the Enter Registration Key page, type or copy the ServerProtect **Registration Key**, and then click **Continue**.
  - **d.** On the Confirm License Terms page, read the license agreement, and then click **I accept** to agree to the terms of the license agreement.
  - **e.** On the Confirm Product Information page, click **Continue Registration**.
  - **f.** Fill out the online registration form, and then click **Submit**.
  - **g.** Click **OK** twice.

After the registration is complete, Trend Micro sends an Activation Code via email, which you can then use to activate ServerProtect and other Trend Micro services.

Installing ServerProtect

This version of ServerProtect for Linux comes prepackaged with Kernel Hook Modules (KHM) for the following kernel:

- 2.4.9-e.3, 2.4.9-e.12
- 2.4.21-4.EL.

Note: Performing an installation requires logging on as root.

To install ServerProtect kernel-dependent mode:

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

   ```
   ./SProtectLinux-1.3.{platform}.i686.bin
   ```

   Where `{platform}` can be any of the following distributions:

   - `RedHat` for Red Hat Enterprise Linux
   - `Turbo` for Turbolinux

   Note: To install ServerProtect in silent mode, type:
   `./SProtectLinux-1.3.{platform}.i686.bin -s`

   The above command extracts the required files in their proper locations.
3. Activate ServerProtect using any of methods found in *Activating ServerProtect* on page 2-9.

To install ServerProtect kernel-independent mode:

1. Check that ServerProtect supports your kernel. Go to the following URL:

   `www.trendmicro.com/en/products/file-server/sp-linux/use/kernel.htm`
2. Click the operating system/processor that corresponds to your Linux server.

3. Click the appropriate Kernel Hook Module (KHM) package for your kernel version.

   For example, the KHM name for kernel 2.4.20-27.8.0 should be:

About KHM versions
KHM names are self-descriptive.

   ```
   SPLX_kernel_module-1.3-1.rh8.0up_2.4.20-27.8.0.i686.tar.gz
   ```

   Where:

   - `SPLX_kernel_module` is the product name
   - `1.3` is the SPLX version
   - `1` is the Kernel Hooking Module release number
   - `rh8.0` is the platform/distribution name and version
   - `up` is the single processor mode
   - `smp` is the symmetric processors mode
   - `2.4.20-27.8.0` is the supported kernel release
   - `i686` is the supported CPU
   - `tar.gz` is the tarball file format

   Supported platforms and CPUs are:

   - `rh` for Red Hat Linux normal version
   - `ra` for Red Hat Linux Enterprise AS (Advanced Server) version
   - `i686` for Intel Pentium
   - `athlon` for AMD Athlon

4. Read the license agreement; if you agree, click **Yes, I accept**.
5. Click **Download now** to download the KHM package.
6. 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-1.3.{platform}.i686.bin
   ```

   Where `{platform}` can be any of the following distributions:

   - `RedHat` for Red Hat Enterprise Linux
   - `Turbo` for Turbolinux

Note: To install ServerProtect in silent mode, type:
`./SProtectLinux-1.3.{platform}.i686.bin -s`

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

7. Copy the KHM package to the following directory:

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

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

   For example:

   ```
   tar xzvf
   SPLX_kernel_module-1.3-1.rh8.0up_2.4.20-27.8.0.i686.t
   ar.gz
   ```

   The following files are extracted from the package:

   For single processor:

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

   For symmetric processors:

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

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

   `/etc/init.d/splx start`

10. Activate ServerProtect using any of methods found in *Activating ServerProtect* on page 2-9.

Activating ServerProtect

Use your Registration Key to register ServerProtect and obtain an Activation Code (or serial number) from the Trend Micro Online Registration Web site (`https://olr.trendmicro.com/registration/us/en-us/login.aspx`) to install a full version. Activate ServerProtect to ensure eligibility to receive the latest security updates and other product and maintenance services. After completing the registration, Trend Micro issues an Activation Code you use to activate Trend Micro software and other Trend Micro services.

Note: The serial number that comes with ServerProtect 1.2x can be used to register and activate ServerProtect 1.3.

To activate ServerProtect:

- **During installation** (that is, after the installation script extracts the required files in their proper locations)

  At the Activation Code prompt, you may opt to enter the Activation Code (serial number) or type **Ctrl+D** to install the 30-day evaluation version. Activate later using any of the succeeding methods.

- **After installation**
  - At the Logon Page

    Enter the product Activation Code (or serial number) in the Serial Number field, then click Register.
  - At the Product Registration Page
    1. Select **Registration** > **Product Registration** from the left-hand menu.
    2. Enter the **Activation Code** in the field, then click **Register**.
  - At the Command console
    1. Go to /opt/TrendMicro/SProtectLinux/SPLX.vsapiapp.
    2. Enter the following:
       ```
       splxmain -q <Activation Code>
       ```

Upgrading from ServerProtect 1.2x

Upgrading allows you to preserve existing ServerProtect configuration settings.

Note: Upgrading to this version of ServerProtect is available for ServerProtect 1.2 or 1.25 with Red Hat Enterprise AS 2.1 kernel 2.4.9-e.16 or Red Hat Enterprise Linux AS 2.1AS 2.1 kernel 2.4.9-e.34, respectively.

To upgrade ServerProtect:

1. Log on as root.
2. From the directory containing the ServerProtect Linux installation files, type the following at the command line:

   ```
   ./SProtectLinux-1.3.RedHat.i686.bin
   ```

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

   Note: To install ServerProtect in silent mode, type:
   `./SProtectLinux-1.3.RedHat.i686.bin -s`

Activate ServerProtect using any of methods found in *Activating ServerProtect* on page 2-9.

Converting an Evaluation Version

If you type **Ctrl+D** during installation, setup installs a 30-day evaluation version of the product. To continue using ServerProtect after the evaluation period, register and activate the product.

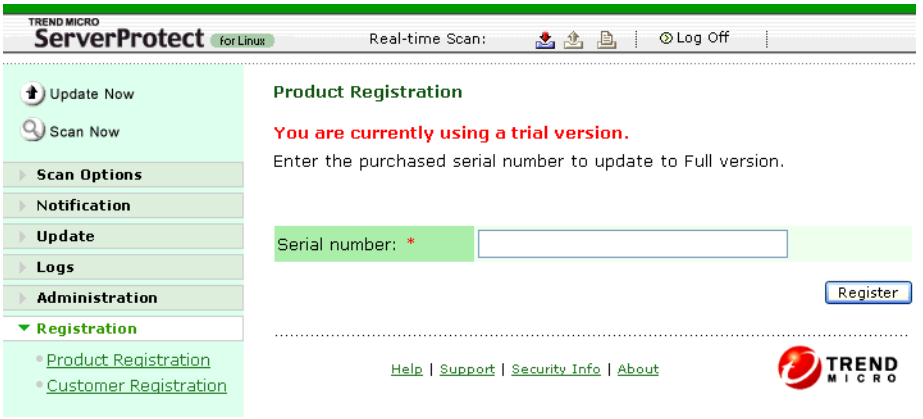


FIGURE 2-1. Product Registration screen

Use the Registration Key included in the ServerProtect package or purchase one from your Trend Micro reseller to obtain an Activation Code (formerly known as serial number) from Trend Micro Online Registration, and then activate ServerProtect using any of the methods found in *Activating ServerProtect* (*After installation* section).

Verifying Installation

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

To verify ServerProtect is running optimally, type the following at the command line:

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

The output should show all running processes, for example:

```
splxmod module is running...
vsapiapp (pid 3854 3852 3851 3850 3849 3840) is running...
entity (pid 3845 3844) is running...
ServerProtect for Linux core is running
splxhttpd (pid 3869 3868 3867 3866 3865 3864) is running...
ServerProtect for Linux httpd is running
```

If a service appears as "stopped", review the installation process.

Removing ServerProtect

Before removing ServerProtect, log on as root.

To remove ServerProtect:

Type the following at the command line:

```
rpm -e SProtectLinux
```

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

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 by searching for each of the following topics in the online help.

This chapter discusses the following topics:

Testing ServerProtect Installation

The European Institute of Computer Antivirus Research (EICAR), in cooperation with antivirus vendors, has developed a test file to check if your system can 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, Trend Micro scan engine will detect it.

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
*
```

Starting and Stopping ServerProtect

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

Note: By default, ServerProtect starts whenever you turn on the server hosting it. It is, however, possible to change this setting. For details see *Configuring Start-up Settings on page 3-4.*

Starting ServerProtect

There are two ways to start ServerProtect: from the command line, or from the XWindow Quick Access console.

Note: Starting ServerProtect requires logging on as root.

To start ServerProtect from the command line:

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

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

   The message "ServerProtect for Linux is running" appears.

To start ServerProtect from the Quick Access console:

1. Log on as a root.
2. From the task bar on the XWindow main window (KDE 2.2.2-2 or higher), click **Start Applications Menu** > **System Tools** > **SPLX Administration** > **Services** > **Start SPLX Service**.

Stopping ServerProtect

There are two ways to stop ServerProtect:

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

Note: Stopping ServerProtect requires logging on as root.

To stop ServerProtect from the command line:

Type the following:

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

To stop ServerProtect from the XWindow Quick Access console:

1. Log on as a root.
2. From the task bar on the XWindow main window (KDE 2.2.2-2 or higher), click **Start Applications Menu** > **System Tools** > **SPLX Administration** > **Services** > **Stop SPLX Service**.

Configuring Start-up Settings

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

To configure start-up settings:

1. Log on as root, and then type **setup** from the command line. The Text Mode Setup Utility appears.
2. Scroll down to **System services management**, then press Enter. The Services window appears.
3. Scroll down to **splx**, and then press the space key to select or deselect it.
4. Select **Ok** for changes to take effect at next server restart.
5. Select **Quit** to close Text Mode Setup Utility.

ServerProtect Web Console

You can use both the Web-based console and the command prompt to configure ServerProtect. The console permits local and remote, as well as multiple-user control of the application via Microsoft Internet Explorer, and Mozilla. See *Supported Web browsers for ServerProtect Web console* on page 2-3 to check which browsers are compatible with ServerProtect.

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

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

To access the Web console:

1. Do one of the following:
   - From the task bar on the XWindow main window (KDE 2.2.2-2 or higher), click **Start Applications Menu** > **System > TrendMicro SPLX Administration > Launch Web Console**.

     Note: Accessing the Quick Access console requires logging on as root.

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

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

     `https://{host name}:14943/`

     Where:

     `{host name}`– is either the computer host name or its IP address

     `14942`– is the default http port number used by ServerProtect.

     `14943`– is the default https port number used by ServerProtect.

     Note: To change the port numbers, use splxmain. See *Using splxmain* starting on Page -21.

2. Type the Web console password, then press Enter. The default password is blank.

Note: For protection, change the Web console password after logging in for the first time. To learn how to change the Web console password, see *To configure ServerProtect Web console passwords:* on page 3-6.

To log off from the Web console:

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

Things to Remember About the ServerProtect Web Console

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

To configure ServerProtect Web console passwords:

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

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

Updating Scan Engine and Virus Pattern

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 recommends updating the following files using Trend Micro's Internet-based component update feature– ActiveUpdate:

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

You can perform updates manually, or let ServerProtect perform them according to a schedule. Trend Micro recommends performing a manual update immediately after installation. Only registered users are eligible for scan engine and virus pattern updates; see *Registering ServerProtect* on page 2-4.

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

To configure proxy settings:

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

Note: To set the proxy password from the command prompt, refer to *Using splxmain* on page A-21.

Configuring a Manual Update

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

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

To use the saved settings do one of the following:

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

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 update component. The current version of each component appears to the right of the component label.

Components to Update

	Component	Current Version
☑	Virus Pattern	474
☑	Scan Engine	6.51

FIGURE 3-1. Components to update

3. Select a download source.

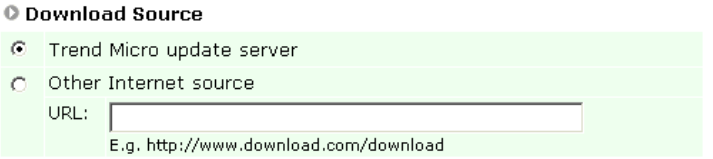


FIGURE 3-2. Download source

Select one of the following download source:

- Trend Micro update server– the default update server

  ServerProtect implements digital signature checking whenever it downloads components from the ActiveUpdate server.

- Other Internet source– specify HTTP or HTTPS Web site (for example, your local Intranet Web site), including the port number that should be used from where ServerProtect can download updates

  The update components have to be available on the primary update source (Web server). Provide the host name or IP address, and directory (for example, `https://12.1.123.123:14943/source`).

  In addition, you can set up multiple backup update servers/sources to automatically fail over in case the primary update source fails.

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

4. Click **Save & Update**.

Configuring a Scheduled Update

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

To configure a scheduled update:

1. Select **Update** > **Scheduled Update** on the left-hand menu. The Scheduled Update screen appears.
2. Select the **Enable Scheduled Update** check box.
3. Select the check box of the update component. 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.
7. Click **Save**.

Configuring and Performing scans

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

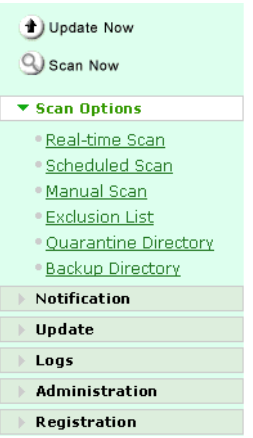


FIGURE 3-4. ServerProtect Web console left-hand menu– Scan Options

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

The scan types are explained below:

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

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

Note: To find out more about the scanning technologies ServerProtect employs, see to *How ServerProtect for Linux works* on page 1-7.

Understanding Virus Actions

You can perform a variety of actions on detected viruses. These appear below.

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

To specify locations to scan:

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

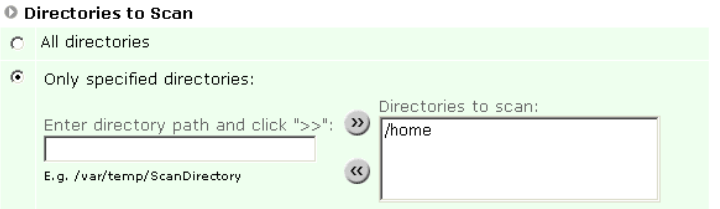


FIGURE 3-5. Directories to scan

The options are:

- **All directories**– scans all directories, except those included in the Exclusion List. For additional information on the Exclusion List, refer to *What is the Exclusion List?* in the online help.

- **Only specified directories**– limits the scan to the directories and subdirectories that you specify. To do so, do the following:

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

  ii. Click  to add the entry to the **Directories to Scan** list.

  iii. Add other directories as required.

  To remove directories that you previously specified:

  i. 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.

  ii. Click  to remove the selected entry.

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

Specifying Files to Scan

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

To specify files to scan:

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

2. Under **File Types to scan**, click the desired scan coverage.

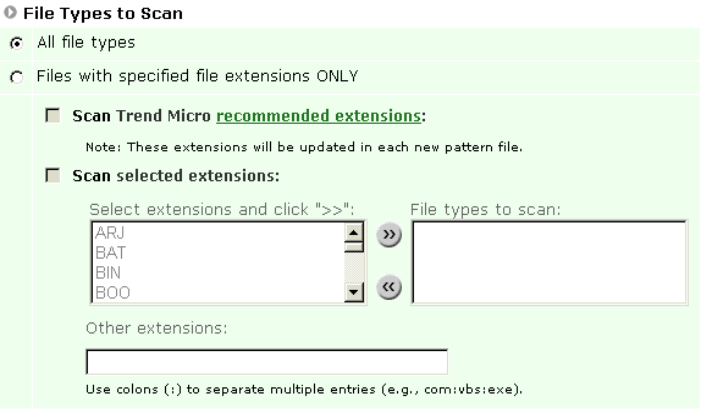


FIGURE 3-6. File types to scan

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 *What is the Exclusion List?* in the online help.
- **Files with specified file extensions ONLY** - Restricts scanning to selected file extensions. This option also has three sub-options, which you can enable either individually or in combination. These are:
  - **Scan Trend Micro recommended extensions** - This option takes advantage of the constantly updated extensions list embedded within the virus pattern.
  - **Scan selected extensions** - You can specify extensions from a list of extensions. To do so, do the following:

  i. 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

  ii. Click  to add the extension to the **File Types to Scan** list.

  To remove previously excluded extensions:

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

ii. Click « to remove the extension from the **File Types to Scan** list.

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

```
LGL;FIN;ADM
```

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

Scanning Compressed Files

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

To scan compressed files:

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

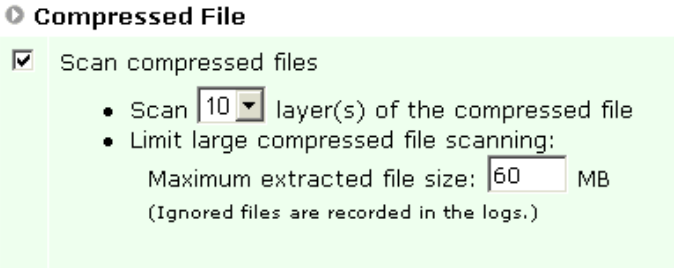


FIGURE 3-7. Compressed file scanning

3. Specify the number of scanning layers to scan. The permitted values are from 1 to 20 layers. The default settings are 5 layers for manual and scheduled scanning, and 1 layer for Real-time scanning.
4. Specify the maximum file size to extract 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 Scan and scheduled scan.

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 3-12.
- **File Types to Scan**– Choose to scan specific file types; see *To specify files to scan:* on page 3-13.
- **Action When Viruses are Found–** Click the appropriate action (clean, quarantine, rename, delete, or pass) ServerProtect should take when it detects a virus, or other malware; see *Understanding Virus Actions* on page 3-12 for details of each action.

Note: On rare occasions, a virus may damage a file in a way that does not allow cleaning and as a result, the infected file is not recoverable. To create a backup copy before ServerProtect attempts to clean it, select the **Back up files to a specified folder before cleaning** check box.

- **Compressed File**– You can perform Real-time scan on compressed files and archives; see *To scan compressed files:* on page 3-15.

Setting Scan Target

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

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

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

FIGURE 3-8. Title bar showing Real-time Scan with incoming, outgoing, and running file scanning enabled

The icons are shown below:

Scan Target	On	Off
Incoming		
Outgoing		
Running		

To specify the scanning direction for Real-time Scan:

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

Invoking Manual Scan (Scan Now)

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

To use the saved settings do one of the following:

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

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 3-19.
3. Click **Save & Scan**. The following confirmation window appears.

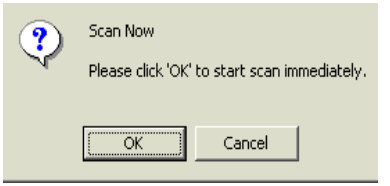


FIGURE 3-9. Scan Now confirmation window

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

To invoke manual scan through the command line:

Run the following command:

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

Where <directory> is the directory you want to scan. Use colon to separate multiple entries. For example, to scan `/temp1` and `/temp2`:

```
splxmain -m /temp1;/temp2
```

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

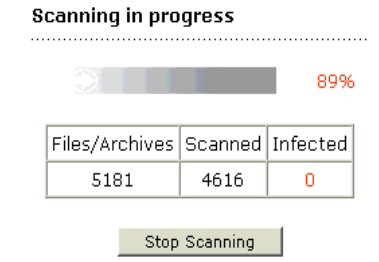


FIGURE 3-10. Scan progress window

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

To stop a manual scan, do one of the following:

- Click **Stop Scanning** on the scan progress screen.
- From the task bar on the XWindow main window, click **Start Applications Menu** > **System Tools** > **SPLX Administration** > **Manual Scan** > **Stop Scan Now**.

Manual Scan Options

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

- **Directories to Scan**– restrict scanning to only specific directories. see *To specify locations to scan:* on page 3-12.
- **File Types to Scan–** limit scanning to specific file types. see *To specify files to scan:* on page 3-13.
- **Action When Viruses are Found–** select the appropriate action (clean, quarantine, rename, delete, or pass) ServerProtect should take when it detects a

virus, or other malware; see *Understanding Virus Actions* on page 3-12 for details about each action.

Note: On rare occasions, a virus may damage a file in a way that does not allow cleaning and as a result, the infected file is not recoverable. To create a backup copy before ServerProtect attempts to clean it, select the **Back up files to a specified folder before cleaning** check box.

- **Compressed File**– perform a manual scan on compressed files and archives; see *To scan compressed files:* on page 3-15.

Configuring a Scheduled Scan

Scheduled scanning is similar to manual scanning, except it follows a schedule you specify.

Enabling Scheduled Scan

Trend Micro recommends enabling scheduled scanning to keep servers free of viruses.

To enable scheduled scan:

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

Invoking Scheduled Scan

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

To invoke scheduled scan:

Issue the following splxmain command from the command line:

```
splxmain -s
```

Stopping Scheduled Scan

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

To stop a scheduled scan:

1. Log on as root.
2. From the task bar on the XWindow main window, click **Start Applications Menu** > **System Tools** > **SPLX Administration** > **Scheduled Scan** > **Stop Scheduled Scan**.

Note: Stopping a running scheduled scan will not disable successive scheduled scans.

Scheduled Scan Options

Scheduled scan has the following scanning options:

- **Directories to Scan**– restrict scanning to only specific directories; see *To specify locations to scan:* on page 3-12.
- **File Types to Scan–** limit scanning to specific file types; see *To specify files to scan:* on page 3-13.
- **Action When Viruses are Found**– select the appropriate action (clean, quarantine, rename, delete, or pass) ServerProtect should take when it detects a virus, or other malware; see *Understanding Virus Actions* on page 3-12 for details about each action.

  Note: On rare occasions, a virus may damage a file in a way that does not allow cleaning and as a result, the infected file is not recoverable. To create a backup copy before ServerProtect attempts to clean it, select the **Back up files to a specified folder before cleaning** check box.

- **Compressed File–** ServerProtect can perform a scheduled scan on compressed files and archives; see *To scan compressed files:* on page 3-15.

Scan Frequency

You can schedule how often ServerProtect scans your computer.

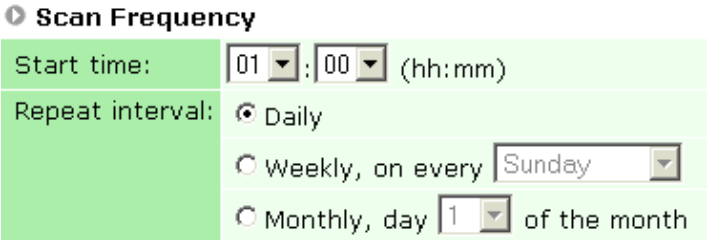


FIGURE 3-11. Scan Frequency

To specify the scan frequency:

Provide the following information:

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

Viewing Scan Results (Logs)

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.

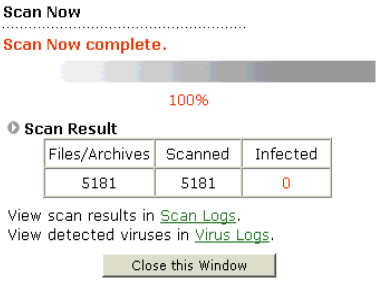


FIGURE 3-12. Scan Now complete window

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

Viewing Scan and Virus Logs

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

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

To view these logs:

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

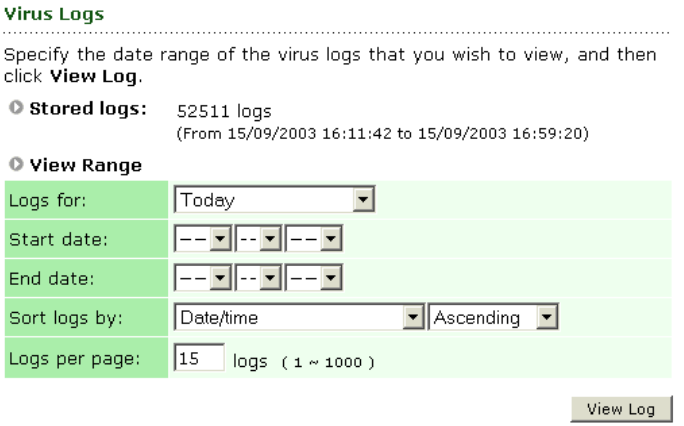


FIGURE 3-13. Virus logs

2. Specify the query criteria for the desired logs. The parameters are:
   - **Logs for**– select among the commonly specified date ranges: **All dates**, **Today**, **Yesterday**, **Past 7 days** or **Past 30 days**. If the period you require is not covered by the above options, choose **Specified date range**; this enables the Start and End date fields.
   - **Start date**– type the earliest log you want to view. Select the **Specified date range** option in **Logs for** to use this criterion. The month-day-year format is used.
   - **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 display 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 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 at the Backup Directory screen. The default location is:

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

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

To specify a Backup Directory:

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

3. Click **Save**.

Note: If you change the location of this directory, existing files will still remain in the original location. After specifying a backup directory, ServerProtect will add it to the exclusion list.

Configuring Notifications

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

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

Setting Alert Events

Specify the alert events and the messages ServerProtect will send for each of them. 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 desired alerts:
   - **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.
   - **Enable Real-time scan configuration change notification**– this sends out a notification whenever a user modifies the Real-time Scan settings.
   - **Enable ServerProtect On /Off notification**– this sends out a notification whenever a user starts or stops ServerProtect service.

- **Enable virus pattern out-of-date notification**– this sends out a warning if the 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 labeled "message" under the different alert events.

Specifying 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 `192.168.0.0`

3. Specify the desired port 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 available.

---

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 common character sets, see *SMTP Mail Notification Character Sets* on page A-27.
- 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

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

This chapter discusses the following topics

Troubleshooting

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

Default password

ServerProtect for Linux does not have a default password. Trend Micro strongly advises 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's customized Apache server does not respond** - Check splxhttpd status. For additional information, see *Using splxhttpd Script* on page A-25.
- **Your 30-day trial period has expired** - If you do not register ServerProtect within 30 days, the Web console will lock out. If this happens, obtain a serial number for your product, then type it in the **serial number** field at the logon screen.
- **Java plug-in not installed properly** - This may happen if you are using Mozilla browser.

Dependency failure during installation

Error message:

```
Dependency failed:
Please install compat-libstdc++ package
```

Solution:

Install the following Red Hat package manager (RPM) package:

```
compat-libstdc++-7.3-2.96.122.i386.rpm
```

Note: The above RPM is available on Red Hat Enterprise Linux 3 AS disc #3. For other supported distribution, please lookup the corresponding package on distribution discs.

Debugging ServerProtect

ServerProtect 1.3 provides the following debug options:

- Kernel debugging– debugs kernel-related actions
- User debugging– debugs user-related actions

Debug Levels

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

VALUE	`UserDebugLevel`	`KernelDebugLevel`
0	Debugging disabled	Debugging disabled (default)
1	Error debugging– logs error messages (default)	Error debugging
2	Information debugging– logs error and warning messages	Common debugging
3	Common– logs error, warning, and notification-type messages	Detailed debugging
4	Critical debugging– logs error, warning, notification, and information-type messages	n/a
5	Detailed debugging– logs error, warning, notification, information, and debug messages	n/a

Note: `UserDebugLevel` does not control output from startup scripts. They will always be logged regardless of UserDebugLevel value.
Detailed debugging produces a large debug file. Trend Micro recommends enabling detailed debugging when replicating an issue, and immediately disabling it after issue replication.

Enabling Debugging

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

To enable debugging:

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

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

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

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

      For example:

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

        ```
        local3.*                /path/splx.log
        ```

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

        ```
        local3.*                /path/splx.debug
        ```

2. Press ESC, and then type the following to save and close the configuration file:

   ```
   :wq!
   ```

3. Query syslogd PID:

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

4. Reload syslogd configuration:

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

5. Restart ServerProtect service:

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

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

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

Disable Debugging

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

To disable debugging:

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

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

2. Press ESC, and then type the following to save and close tmsplx.xlm:

   ```
   :wq!
   ```

3. Delete or comment out the debug path and filename in `/etc/syslog.conf`.
4. Restart ServerProtect service:

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

5. Query syslogd PID:

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

6. Reload syslogd configuration:

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

Before Contacting Technical Support

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

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

  To search the Knowledge Base, visit

  `http://kb.trendmicro.com/solutions/solutionSearch.asp`

Contacting Technical Support

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

- Email support

  `support@trendmicro.com`

- Help database- configuring the product and parameter-specific tips
- Readme- late-breaking product news, installation instructions, known issues, and version specific information
- Knowledge Base- technical information procedures provided by the Support team:

  `http://kb.trendmicro.com/solutions/solutionSearch.asp`

- Product updates and patches

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

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

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

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

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

Sending infected files to Trend Micro

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

`subwiz.trendmicro.com`

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

TrendLabs™

Trend Micro TrendLabs is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

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

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

For more information about TrendLabs, please visit:

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

Other Useful Resources

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

Internet-based tools and services include:

- Virus Map- monitor virus incidents around the world
- HouseCall™- Trend Micro online virus scanner

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

Appendix

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

This chapter discusses the following topics:

Accessing ServerProtect Man Pages

ServerProtect man pages contain relevant ServerProtect command and configuration information.

ServerProtect man pages are:

- `tmsplx.xml`– explains the ServerProtect configuration parameters
- `splxmain`– includes the splxmain command information
- `splx`– explains the ServerProtect startup script and includes error messages

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

```
man {manpage}
```

For example:

```
man tmsplx.xml
```

Understanding `tmsplx.xml`

This section includes descriptions of the parameters for configuring ServerProtect.

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

The configuration file is located in:

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

Entries adhere to the following format:

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

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

- Scan Group Keys
- ActiveUpdate Group Keys
- SOURCEINFO Group Keys

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
- Logs Group Keys

The criteria for editing the configuration file are:

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

  For example:

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

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

To restart ServerProtect, type the following at the command line:

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

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

Note: Whenever you replace an existing configuration file with the `tmsplx.xml.tmplate` file, the ServerProtect Web console will require re-applying your Activation Code (also referred to as serial number). This is because the Activation Code is stored in the configuration file.

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

Scan Group Keys

This set of keys control virus-scanning operations. You can configure Real-time Scan, scheduled scan, and manual scan individually.

Scheduled scans run at predetermined times through `cron`; ServerProtect converts the frequency and time information specified in the `tmsplx.xml` file into valid `crontab` entries. You can specify to scan files by directory, or by extension, using either a "scan all files except the specified ones" or a "do not scan any files other than the specified ones" logic.

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

`RealtimeScan`

This key enables/disables Real-time Scan.

The valid values are:

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

`RealtimeIncludeDirList`, `ScheduledIncludeDirList`, `ManualIncludeDirList`

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

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

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

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 enable/disable scanning of file types (identified by extension) that Trend Micro recommends scanning. The valid values are:

- `0` do not use this list
- `1` use this list (default value)

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 value is:

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

RealtimeExcludeFileList, ScheduledExcludeFileList, ManualExcludeFileList

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

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

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

RealtimeExcludeExtList, ScheduledExcludeExtList, ManualExcludeExtList

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

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

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

RealtimeAction, ScheduledAction, ManualAction

Use these keys to define an action when ServerProtect finds a virus. The valid values are:

`ACTION_CLEAN`

Attempt to clean the file of the virus. This is the default value.

`ACTION_MOVE`

Move infected files to the quarantine directory specified by the `DirToMove` key.

`ACTION_RENAME`

Rename infected files by appending the extension specified by the `FileExtentionToRename` key.

`ACTION_DELETE`

Delete infected files.

`ACTION_BYPASS`

Take no action when ServerProtect detects a virus.

`RealtimeActionAfterCleanFail`, `ScheduledActionAfterCleanFail`, `ManualActionAfterCleanFail`

Action to take if ServerProtect finds a virus, however cannot clean the infected file. The valid values are:

- `ACTION_MOVE` (default)
- `ACTION_RENAME`
- `ACTION_DELETE`
- `ACTION_BYPASS`

`RealtimeScanArchived`, `ScheduledScanArchived`, `ManualScanArchived`

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

`0` disable scan of archived files

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

`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 number of compression layers ServerProtect scans. The valid values are `1` through `20`; the default value for Real-time Scan is `1`.

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 you wish to scan. This value is in megabytes; the maximum value is `2000`; 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 (default)

`1` enable file backup

DirToMove

This key shows the directory where infected files go when ServerProtect finds a virus and the `Action` or `ActionAfterCleanFail` keys are set to `ACTION_MOVE`. 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
```

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`, the default value is `100`. This key has no effect if the `VirusOutbreak` key is disabled.

AlertVirusInfection

This key enables/disables the functionality of sending an alert notification when ServerProtect 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 enables/disables the functionality of sending 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)

AlertServerProtectOnOff

This key enables/disables the functionality of sending an alert notification whenever **splx** service stops or restarts. The valid values are:

`0` disable sending an alert notification whenever **splx** service stops or restarts

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

AlertPatternOutOfDate

This key enables/disables the functionality of sending an alert notification whenever the pattern file is out-of-date.

`0` disable sending an alert notification whenever the pattern file is out-of-date

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

AlertPatternOutOfDatePeriod

This key sets the frequency, in days, for checking the pattern file is up-to-date (current). The valid values are `1` though `1000`; the default value is `60`. For example, to have ServerProtect check the pattern file is current once every `70` days, type the following:

```
<P Name="AlertPatternOutOfDatePeriod" Value="70"/>
```

Schedule

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

`0` no scheduled scan jobs (default value)

`1` scheduled scan jobs run once every hour

`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).

Note: If the value of the Schedule key is `1` (once a every hour), ServerProtect will ignore the hour portion of this time.

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`; the default value is null.

ScheduledMDay

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

ScheduledNOption

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

`0` do not update any components

- `1` update virus pattern
- `2` update scan engine
- `3` update virus pattern and scan engine (default value)

ManualNOption

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

- `0` do not update any components
- `1` update virus pattern
- `2` update scan engine
- `3` update virus pattern and scan engine (default value)

Schedule

This key specifies the schedule for Scheduled updates. The valid values are:

- `0` no schedule (default)
- `1` hourly updates
- `2` daily updates
- `3` weekly updates
- `4` monthly 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`, `3`, or `4`.

ScheduledWDay

This key specifies the day of the week for scheduled updates, when the value of the `Schedule` key is `3`. The valid values are: `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`, and `Sunday` (default).

ScheduledMDay

This key specifies the day of the month for scheduled updates when the value of the `Schedule` key is `4`. The valid values are `1` through `31`. The default value is `1`.

SOURCEINFO Group Keys

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

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 (default)

SrvAuth

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

- `0` disable digital signature download (default)
- `1` enable digital signature download

Merge

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

- `0` disable digital signature download
- `1` enable digital signature download (default)

Source

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

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

Port

This key contains the port number of the ActiveUpdate URL defined in the `Source` and `DefaultSource` keys. The default value is `80`.

ProxyUsername

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

ProxyPassword

If your proxy server requires authentication, this key contains the password. The default value is null. You can modify this value using the Web console and splxmain. See *Using splxmain* on page A-21.

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.

Notification Group Keys

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

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

Type

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

"" (null) default value

SMTP use an SMTP server

SNMP use the SNMP protocol

SMTP:SNMP use both delivery methods

SmtpServer

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

```
mail.company.com
```

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

SmtpPort

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

SmtpFrom

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

```
administrator@company.com
```

The default value is null.

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

SmtpTo

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

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

Note: The default value of this key is null.

SmtpCharset

This key specifies the character set ServerProtect uses to encode notification emails. For information on other commonly used character sets. See *SMTP Mail Notification Character Sets* on page A-27 for additional information. The default value is `iso-8859-1` (Latin 1 Western European).

SnmpHostname

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

```
snmp.company.com
```

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

SnmpCommunity

This key contains the SNMP community name. For example:

```
defaultpublic
```

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:

```
Virus outbreak subject
```

VIRUSOUTBREAKMESSAGE

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

```
Virus outbreak message
```

VirusInfectionSubject

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

```
Virus infection subject
```

VIRUSINFECTIONMESSAGE

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

```
Virus infection message
```

RealtimeConfigChangeSubject

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

```
Realtime configuration change subject
```

REALTIMECONFIGCHANGEMESSAGE

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

```
Realtime configuration change message
```

ServerProtectOnOffSubject

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

```
ServerProtect on/off subject
```

SERVERPROTECTONOFFMESSAGE

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

```
ServerProtect on/off message
```

PatternOutOfDateSubject

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

```
Virus pattern out of date subject
```

PATTERNOUTOFDATEMESSAGE

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

```
Virus pattern out of date message
```

Logs Group Keys

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

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

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

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

Schedule

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

- `0` disable automatic deletions of the log file
- `1` hourly deletions
- `2` daily deletions (default value)
- `3` weekly deletions
- `4` monthly deletions

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).

ScheduledWDay

This key specifies the day of the week for log deletions. The valid values are: `Sunday` (default), `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, and `Saturday`.

Note: This key works only when the value of the `Schedule` key is `3` (weekly deletions).

ScheduledMDay

This key specifies the day of the month for log deletions. The valid values are `1` through `31`. The default value is `1`.

Note: This key has no effect unless the value of the `Schedule` key is `4` (monthly deletions).

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.

Using splxmain

The splxmain command enables you to maintain and control ServerProtect from the command line. Running splxmain requires root privileges.

Note: You should only use splxmain if you wish 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 |-E |-f |-g <date> |-i |-j |-k |-l |-m
<directory> |-n |-o |-p |-q <Activation Code> |-r |-s |-t |-u
|-v |-w <port> |-x |-y ][-D ]
```

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

Parameters:

- -a terminates all virus scan daemon (vsapiapp) processes gracefully. To kill these processes immediately, use the -k option (not recommended).
- -b removes all scheduled jobs from crontab, letting current jobs complete first.
- -c refreshes the scheduled scan, scheduled update, and scheduled log deletion settings, based on the settings in the tmsplx.xml file. Run this command after making changes to the tmsplx.xml file to make the relevant crontab changes.
- -D forces vsapiapp to run as a daemon. This option can be used with -e.
- -e reads the tmsplx.xml(5) configuration file and sets up the crontab(5) tables to run Scheduled Scans, Scheduled Updates, and Automatic Log Purges, then launch vsappiapp.

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

`-E` checks the remaining days left before the 30-day evaluation version expires.

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

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

```
splxmain –g 2003-05-21 # deletes logs older than May 21, 2003
```

Note: If you do not specify `<date>`, ServerProtect will use the value of the `MaxLogDay` key in the `tmsplx.xml` file. See *MaxLogDay* on page A-20.

`-i` restarts all vsapiapp processes.

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

`-k` terminates vsapiapp processes, manual scan processes, and scheduled scan processes immediately by sending a `SIGKILL` signal. To have less impact on the system, first, try to terminate these processes using the `-a` option.

`-l` sets the SPLX HTTP port for accessing the SPLX Web console. For example, `splxmain -l 14942`

`-m <directory>` executes a manual scan immediately, 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` terminates the manual scan process currently running.

`-o` disables the scheduled scan, by removing only the scheduled scan commands from the `crontab` file.

`-p` triggers the Scheduled Upate process

`-q <Activation Code>` sets the Activation Code (or serial number).

`-r` reloads the SPLX configuration without restarting vsapiapp.

`-s` executes the Scheduled scan immediately, based on the scheduled scan settings in the `tmsplx.xml` file. Normally, you should use the `-m` option to run an on-demand scan; ServerProtect uses this option in the `crontab` file.

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

`-t` terminates the scheduled scan process currently running.

`-u` updates the virus pattern and scan engine according to the settings in the `ActiveUpdate` and `SOURCEINFO` groups in the `tmsplx.xml` file. After updating, ServerProtect will reload the engine and pattern.

`-v` enables Real-time Scan by spawning child processes. Scanning will start according to the Real-time Scan settings in the `Scan` group of `tmsplx.xml`.

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

```
splxmain -w 14943
```

`-x` disables Real-time Scan by terminating the Real-time Scan child processes.

`-y` sets the proxy password.

Using splx Script

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

Location:

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

Syntax:

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

Parameters:

`start`

Starts the ServerProtect service and the ServerProtect Apache server

`stop`

Stops the ServerProtect service and the ServerProtect Apache server

`restart`

Stops, and then restarts the ServerProtect service and the ServerProtect Apache server

`status`

Displays currently active ServerProtect threads

Using splxcore Script

Use **splxcore** script to run ServerProtect without Apache server.

Note: Use splxcore script to manage ServerProtect exclusively from the command line (no Web console).

Location:

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

Syntax:

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

Parameters:

`start`

Starts the ServerProtect core service

`stop`

Stops the ServerProtect core service

`restart`

Stops, and then restarts the ServerProtect core service

`status`

Displays currently active ServerProtect core processes

Using `splxhttpd` Script

Use **splxhttpd** script to enable/disable Apache server.

Location:

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

Syntax:

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

Parameters:

`start`

Starts ServerProtect Apache server

`stop`

Stops the ServerProtect Apache server

`restart`

Stops, and then restarts the ServerProtect Apache server

`status`

Displays currently active ServerProtect Apache processes

Using `splxcomp` Script

The ServerProtect package comes with a tool that is designed to address certain customization issues. The `splxcomp` tool can be found in the following directory:

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

`splxcomp` prevents redundant scanning when installing Trend Micro InterScan™ VirusWall™ for Linux and ServerProtect on the same server. Use `splxcomp` to locate and exclude InterScan VirusWall for Linux quarantine and backup directories.

Note: Use this tool only when installing InterScan VirusWall for Linux and ServerProtect on the same server.

Syntax:

```
splxcomp {-h} {-v} {-i}
```

Parameters:

- `-h` displays the tool's parameters list
- `-v` displays version information
- `-i` obtains critical settings from Trend Micro InterScan VirusWall

Apache Configuration File

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

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

WARNING! *Editing the customized Apache server configuration file may result in unexpected errors. Before making any changes to this file, back up* `splxhttpd.conf` *to restore your original settings. Contact Trend Micro Support for help when editing* `splxhttpd.conf`.

Apache Log Files

You can find ServerProtect Apache server log files in the following directory:

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

SMTP Mail Notification Character Sets

The following is a sampling of the character sets, which ServerProtect supports. For information on how these character sets are used; see *To enable SMTP mail notification:* on page 3-29.

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

Index

S