TREND MICRO™

3.0 ServerProtect™

Getting Started Guide

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

for Red Hat Enterprise Linux v8&CentOS v8&SUSE 15

Endpoint Security

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 applicable user documentation, which are available from the Trend Micro Web site at:

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

Trend Micro, the Trend Micro logo, InterScan VirusWall, MacroTrap, ServerProtect, Apex Central, Control Manager, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2019 Trend Micro Incorporated. All rights reserved.

Document Part No. SPEM38858/191118

Release Date: November 2019

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

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

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

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

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

Contents

Preface

Audience P-2

ServerProtect Documentation P-2

Document Conventions P-3

Chapter 1: Pre-Installation

System Requirements 1-2

Information Needed to Install ServerProtect 1-3

Chapter 2: Installation

ServerProtect Installer Options 2-2

Local Installation Procedure 2-3
- Running the ServerProtect Installation Program 2-3
- Accepting the Trend Micro End User Agreement 2-4
- Registering ServerProtect to Control Manager 2-5
- Activating ServerProtect During Installation 2-7

Remote Installation 2-8
- Extracting RemoteInstall From the ServerProtect Binary 2-9
- Using a Configuration File in Your Remote Deployment 2-10
- Running the RemoteInstall Tool 2-14

Kernel Hook Module 2-16
- Installing a Kernel Hook Module Package 2-17

Verifying the Installation 2-19

Uninstalling ServerProtect 2-19

Chapter 3: Post Installation Configuration

Logging On to the ServerProtect Web Console 3-2

Setting Up an Administrator Password 3-3

Configuring Proxy Server Settings 3-4
General Proxy Settings 3-4
Component Update Proxy Settings 3-5

Registering ServerProtect 3-7

Activating ServerProtect 3-8

Upgrading to the Full Version 3-9

Updating Components 3-12
Initiating Automatic Update on Control Manager 3-12

Testing ServerProtect with the EICAR Test Virus 3-12

Configuring rsyslog 3-13

Appendix A: Building and Installing Kernel Hook Module

Introduction A-2

Requirement A-2

Installation A-3

Appendix B: Troubleshooting and Contacting Technical Support

Troubleshooting B-2
Problem with Missing Dependent Libraries in Linux B-2
Building and Installing KHM B-2
Default Password B-4
Web Console Rejects Passwords B-4
Debug Logs B-4

Before Contacting Technical Support B-4

Contacting Technical Support B-5

About TrendLabs B-6
About Software Updates B-6
Known Issues B-7

Other Useful Resources B-8
About Trend Micro B-9

Index

Preface

Preface

Welcome to the Trend Micro™ ServerProtect™ for Linux 3.0 (SPLX3.0) Getting Started Guide. This guide contains basic information about the tasks you need to perform to install the product and basic configuration. This preface discusses the following topics:

- *Audience* on page 2
- *ServerProtect Documentation* on page 2
- *Document Conventions* on page 3

Audience

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

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

ServerProtect Documentation

The ServerProtect for Linux 3.0 documentation consists of the following:

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

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

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

Document Conventions

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

TABLE 1.

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

Chapter 1

Pre-Installation

This chapter guides you through the information gathering phase before installing ServerProtect for Linux (SPLX) on your Linux server.

This chapter discusses the following topics:

- *System Requirements* on page 1-2
- *Information Needed to Install ServerProtect* on page 1-3

System Requirements

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

Hardware

Processor

- Intel™ Pentium™ II or higher
- AMD Athlon™ or higher

Note: This version of ServerProtect supports Intel processors with Intel 64 architecture and AMD processors with AMD64 technology. Intel Itanium architecture is not supported.

Memory

- 512-MB or more (1-GB recommended for application/file servers)

Disk space

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

Software

Supported Distributions and Kernels

- Red Hat Enterprise Linux 8 (x86_64):
  - 4.18.0-80.el8.x86_64
- CentOS Linux 8 (x86_64):
  - 4.18.0-80.el8.x86_64
- SUSE Linux Enterprise Server 15 (x86_64):
  - 4.12.14-23.1.x86_64
  - 4.12.14-195.1.x86_64

For other kernels and distributions, refer to the following Web site for additional information:

```
http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=111&regs=NABU&lang_loc=1
```

Supported Web Browsers

Access the ServerProtect Web console through either of the following:

- Microsoft™ Internet Explorer™ 11.0 or later

Note: If you use Internet Explorer™ 11.0 or later, you must disable the pop-up window blocker feature to display the Web console online help content.

- Mozilla Firefox 37 or higher

Information Needed to Install ServerProtect

The ServerProtect setup program prompts you for the required information, depending on the options chosen during the installation process.

Proxy For Internet Updates

If you have a proxy between the ServerProtect server and the Internet, type the proxy's host name or IP address, port number, and an account user name and password.

Apex Central / Control Manager Server Information

If you plan to register ServerProtect to an existing Trend Micro Apex Central™ / Control Manager™ server on the network, you need to know the server's host name or IP address and its logon name.

Note: To register ServerProtect to the Apex Central / Control Manager server on your network, you need Trend Micro Apex Central or Control Manager Server 7.0.

Activation Code

During product registration, the Registration Key is exchanged for an Activation Code (also known as a serial number) that "unlocks" the program. You can register and obtain the Activation Code before installing by visiting Trend Micro's online registration Web site at:

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

Note: Some resellers may have already registered ServerProtect for you and given you the product serial number directly.

Local or Remote Installation

You can install ServerProtect on either a local or remote server. You can also install ServerProtect to one or more remote servers.

Chapter 2

Installation

This chapter guides you through the installation of ServerProtect on your Linux server(s). This chapter discusses the following topics:

- *ServerProtect Installer Options* on page 2-2
- *Local Installation Procedure* on page 2-3
- *Remote Installation* on page 2-8
- *Kernel Hook Module* on page 2-16
- *Verifying the Installation* on page 2-19
- *Uninstalling ServerProtect* on page 2-19

ServerProtect Installer Options

For details on the parameters you can use with the installer, type the following at the command line:

```
./SProtectLinux-3.0.bin -h
```

The table below describes the parameters.

Option	Description
`-f`	Force-install the ServerProtect for Linux.
`-h`	Display a list of parameters available with this binary (the output that is displaying now).
`-n`	Do not start the ServerProtect service after ServerProtect is installed.
`-r`	Extract remote install tool.
`-s`	Do not show license agreement.
`-S {Activation Code}`	Type the Activation Code to activate ServerProtect.
`-x`	Extract rpm file of ServerProtect for Linux.
`-X`	Extract binary file of ServerProtect for Linux.

Local Installation Procedure

The following lists the steps to install ServerProtect for Linux 3.0 on a local Linux server. The subsequent sections describe these steps in detail.

Step 1. *Running the ServerProtect Installation Program*

Step 2. *Accepting the Trend Micro End User Agreement*

Step 3. *Registering ServerProtect to Control Manager*

Step 4. *Activating ServerProtect During Installation*

Step 5. *Installing a Kernel Hook Module Package* (if required)

Running the ServerProtect Installation Program

Before installing ServerProtect for Linux, verify that your Linux distribution and kernel are supported by this release. (See *Supported Distributions and Kernels* on page 1-2). If your kernel is not listed in the *System Requirements* section in this chapter, follow the procedure in the *Installing a Kernel Hook Module Package* section to install the Kernel Hook Module (KHM) that corresponds to your Linux system.

Note: Before you install ServerProtect on your Linux computer, make sure the following dependent packages are installed. For the versions, you can use the default libs bundled in the OS image.
-glibc
-libgcc
-zlib
-bzip2
-libuuid
-libstdc++ (Red Hat and CentOS only)
-nss-softokn-freebl (Red Hat and CentOS only)
-perl-Sys-Syslog (Red Hat and CentOS only)

To begin ServerProtect installation:

1. Download or copy the ServerProtect for Linux installation files.
2. Log on as *root*.

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

   `./SProtectLinux-3.0.bin`

   This command extracts the required files to their proper locations.

The following procedure shows you how to disable Real-time Scan during installation.

To install ServerProtect with real-time scan disabled:

1. Use the `-n` option to start the installation. For example, type `./SProtectLinux-3.0.bin -n` at the command line.
2. After the installation is complete, set the value of the `RealtimeScan` parameter to 0 in the `tmsplx.xml` configuration file.
3. Restart the ServerProtect service.

Note: If a message displays warning that the KHM does not support your Linux kernel, build and install the KHM. After the KHM installation is complete, do NOT start or restart the ServerProtect service. Then perform steps 2 and 3 as described above.

WARNING! **If you use the `-n` option to install ServerProtect, you must manually configure the ServerProtect service to run at system startup. You can do this by typing "`./add_splx_service`" in the `/opt/TrendMicro/SProtectLinux/SPLX.util` folder.**

Accepting the Trend Micro End User Agreement

Before beginning the installation of ServerProtect, the first task is to review and accept the Trend Micro end user license agreement.

Press the [SPACE] bar to scroll to read the license. When you have finished reading, type "yes" to accept the licensing terms. (If you do not type "yes," installation cannot continue.)

```
NOTICE: Trend Micro licenses its products in accordance with cer-
tain terms and conditions. By breaking the seal on the CD jacket
in the Software package or installing a serial number, registra-
tion key or activation code, You already accepted a Trend Micro
license agreement. A courtesy copy of a representative Trend Micro
License Agreement is included for reference below. The language
and terms of the actual Trend Micro license agreement that you
accepted may vary. By accepting the License Agreement below, or
using the Software, You confirm Your agreement to the terms and
conditions of the original Trend Micro license agreement you
accepted.

Trend Micro License Agreement
(Package Version 0403Nov03E021004)

-----------------------[SNIP] -------------------------

SPLX version 3.0 Released June, 2015

Do you agree to the above license terms? (yes or no)
```

FIGURE 2-1. License agreement acceptance

Registering ServerProtect to Control Manager

Before you can use Trend Micro Control Manager to manage ServerProtect, you may register ServerProtect to Control Manager during the installation process.

To register ServerProtect to Control Manager:

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

   If you do not wish to manage ServerProtect by using Control Manager, type "n" and press [ENTER]. An "`Activate ServerProtect to continue scanning and security updates.`" message displays and ServerProtect

prompts you to type your Activation Code. See *Activating ServerProtect During Installation* on page 2-7 for further guidance on this process.

3. At the `SPLX server name or IP address:` prompt, type the name or IP address of your ServerProtect server.
4. At the `Do you wish to connect to Control Manager server using HTTPS? (y/n) [n]` prompt, type `y` to connect to Control Manager using HHTPS; otherwise type `n` to use HTTP connection.
5. At the `Control Manager server name or IP address:` prompt, type server name or the IP address of the Trend Micro Control Manager server that you want to use to manage ServerProtect.
6. At the `Control Manager server port: [80]` prompt, type the port number that you would like to use to access Control Manager or just press [ENTER] to accept the default value of 80.
7. At the `Do you access Control Manager through a proxy server? (y/n) [n]` prompt, type `y` if you do or just press [ENTER] to accept the default choice of **`n`**. If you choose `n`, the installer asks you to specify the display name to identify ServerProtect on the Control Manager Web console. If you do use a proxy server to connect to Control Manager, see *Proxy Server Information* on page 2-7 for further guidance on this process.
8. At the `Please specify the name you would like to display on the Control Manager console: [SPLX server name or IP address]` prompt, type the desired name. Control Manager will use this name to identify your ServerProtect server on the Control Manager Web console.
9. At the `Please specify a folder name for this product (for example: /SPLX) [New entity]:` prompt, type the folder path. The installer displays a summary of the information you have entered and asks you to confirm your choices.
10. At the `Is the above information correct? (y/n) [n]` prompt, confirm or reject the displayed choices. If you type **`n`** (or just press [ENTER] to accept the default choice of **`n`**), the installer prompts you to re-type all of the above information, starting with the IP of your ServerProtect server. If you type `y` to confirm all of the displayed information, the "Saving information to the configuration file … done" message displays and ServerProtect asks if you would like to type your Activation Code. See *Activating ServerProtect During Installation* on page 2-7 for further guidance on this process.

Proxy Server Information

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

To specify proxy server information during installation:

Type the following information at the corresponding prompts:

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

  (If authentication is required—)

  - Proxy user name:
  - Proxy password:
  - Retype proxy password:

Activating ServerProtect During Installation

If you register and activate the software, a fully licensed ("standard") version of the product will be installed. If you skip registration and activation, the product will not be activated and scan and component update functions will not be enabled. Updates will not resume until you register and activate ServerProtect.

1. You are prompted to register the software. You can do so at this point or skip this step and register later.

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

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

FIGURE 2-2. Prompt to register ServerProtect during installation

   a. To register now, visit the following URL:

```
https://olr.trendmicro.com/redirect/product_register.asp
x
```

b. Follow the steps described in *Registering ServerProtect* starting on page 3-7.

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

   To activate ServerProtect, type the Activation Code at the prompt and press [ENTER].

   See *Registering ServerProtect* on page 3-7 for instructions on registering the ServerProtect if you did not register or activate during installation.

Remote Installation

Many ServerProtect customers install and administer ServerProtect in a centrally managed, distributed environment. Trend Micro provides a remote installation tool (RemoteInstall) for this reason.

RemoteInstall Features

RemoteInstall has the following features:

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

The following lists the steps in performing a remote installation:

1. Extracting RemoteInstall.
2. Editing a RemoteInstall configuration file.
3. Running RemoteInstall.

Extracting RemoteInstall From the ServerProtect Binary

You can use the **-r** parameter to extract RemoteInstall from a single package or from the binary file for a specific Linux kernel version. For example, the following command extracts the remote install tool from the ServerProtect for Linux 3.0 binary file:

```
./SProtectLinux-3.0.bin -r
```

After you have accepted the license agreement and have extracted the remote installation program (RemoteInstall), the above command creates a `remote.install.splx` subdirectory in your working directory. See the following table for a list of files and directories that this subdirectory contains.

TABLE 2-1. RemoteInstall directories

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

Using a Configuration File in Your Remote Deployment

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

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

For brevity, only the most important configurable keys are listed in the table below. For detailed explanations of keys, see the Administrator's Guide.

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

Key	Description
DeployOption	Indicates the type of deployment to perform. Value 1: ServerProtect package deployment and installation Value 2: ServerProtect configuration file update Value 3: KHM deployment
PackageName	Indicates the ServerProtect installation path for package deployment.
Activation Code	Used in package deployment. Value is the ServerProtect Activation Code for installation.
ConfigFilePath	Used in configuration file deployment. Indicates configuration file path.

Converting CSV-Formatted Files to RemoteInstall.conf Format

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

To edit and use RemoteInstall configuration file in CSV format:

1. Import the file `RemoteInstall.csv` to a spreadsheet program and edit the file. Save the file under another name.
2. Copy the new file to your ServerProtect `remote.install.splx` directory.
3. When you run RemoteInstall, use the **`-p`** option followed by the name of the revised CSV file, for example:

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

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

Specifying Clients for Remote Deployment

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

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

Single Deploy

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

TABLE 2-3. Client assignment keys in configuration file, single deploy

Line	Description
1. [x.x.x.x]	IP address of client
2. RootPassword	root password of client
3. ConnectCM	Value 1 (the default): register to Control Manager server. Value 0: do not register to Control Manager server
4. CMServerIP	IP address of Control Manager server
5. CMServerPort	connection port of Control Manager server (default = 80)
6. UseProxyAccessCM	Value 1: use a proxy server to connect to Control Manager server. Value 0 (the default): do not use proxy
7. ProxyServerIP	IP address of proxy server
8. ProxyServerPort	connection port of proxy server (default = 80)
9. ProxyAuthentication	Value 1: use proxy authentication Value 0 (default): do not use
10. ProxyUserName	Proxy authentication user name

TABLE 2-3. Client assignment keys in configuration file, single deploy

Line	Description
11. ProxyPassword	Proxy authentication password
12. CMClientName	Client computer name that displays in Control Manager console. Default = IP address of client
13. CMProductDirectoryName	Directory name that displays in Control Manager console. Directory is used to group clients. Default = “New entity”

Group deploy

For group deployment, all of the lines are identical to those under `#single deploy` except for the following.

TABLE 2-4. Client assignment keys in configuration file, group deploy

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

Tip: For ease of reference, Trend Micro suggests starting any group names with an easily identifiable term, such as *Sales, RD,* and likewise for computer names, for example, *Server1, Server2,* and so on.

Running the RemoteInstall Tool

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

To execute RemoteInstall:

1. Place the ServerProtect full binary file on the deploying server.
2. Extract RemoteInstall from the ServerProtect binary. (See *Extracting RemoteInstall From the ServerProtect Binary* on page 2-9 for details.)
3. To deploy ServerProtect to multiple computers, configure the `RemoteInstall.conf` file for deployment. (See *Running the RemoteInstall Tool* on page 2-14 for detailed guidance on the `RemoteInstall.conf` file.)
4. Issue the following command at the command line:

   ```
   ./RemoteInstall
   ```

   RemoteInstall deploys ServerProtect to the target computer(s) and outputs progress messages. The deployment creates the five results files described in table below.

TABLE 2-5. Results files produced by RemoteInstall

Results File	Description
splx_failed_list_yyyy-mm-dd_hhmmss.conf	failed list for configuration file format
splx_failed_list_yyyy-mm-dd_hhmmss.csv	failed list for `.CSV` file format

TABLE 2-5. Results files produced by RemoteInstall

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

RemoteInstall Tool Options

Use the **`-h`** parameter to display the usage of the RemoteInstall tool options:

```
./RemoteInstall -h
```

TABLE 2-6. Parameters available for use with RemoteInstall script

Parameter	Description
-c	Check client info
-f {alternative_config_file}	Specified configuration file of remote install. Use this option to run RemoteInstall with a configuration file other than `RemoteInstall.conf`. (You can use an alternative configuration file as long as the alternative file contains the same key-value pairs as `RemoteInstall.conf`. See *Using a Configuration File in Your Remote Deployment* on page 2-10)
-h	Show usage

TABLE 2-6. Parameters available for use with RemoteInstall script

Parameter	Description
`-n`	Do not show license agreement
`-p {csv_file}`	Convert specified csv file to configuration file for use with RemoteInstall (see *Converting CSV-Formatted Files to RemoteInstall.conf Format on page 2-10* for detailed guidance on this option)
`-v`	Show version

Kernel Hook Module

This version of ServerProtect for Linux comes prepackaged with a kernel hook module (KHM) for each of the supported kernels. The source code for the kernel hook module is also included in the installation package.

Installation of a KHM is required for ServerProtect to perform real-time scanning. If your Linux kernel is one of those listed in *Supported Distributions and Kernels* on page 1-2, the ServerProtect setup program automatically installed the appropriate KHM that comes prepackaged with ServerProtect.

If your Linux kernel is not listed, do the following:

1. Download the KHM for your Linux kernel from the Trend Micro ServerProtect for Linux Kernel Support Web site:

   `http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=111&regs=NABU&lang_loc=1`

2. If a KHM is not available for your Linux kernel, build the KHM on your Linux system. Refer to *Building and Installing Kernel Hook Module* on page A-1 for instructions.

Note: When you upgrade the Linux kernel, you need to copy the KHM to the directory where ServerProtect is installed.

Installing a Kernel Hook Module Package

This section describes how to install the KHM package you download from the Trend Micro website. You may also install a new, updated KHM after installing ServerProtect.

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

To install the KHM:

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

   `http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=111&regs=NABU&lang_loc=1`

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

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

4. Go to the directory shown above and extract the KHM package using the following command:

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

   The following files are extracted from the package:

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

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

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

   `/etc/init.d/splx restart`

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

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

or

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

Make sure your Linux system port 14942 or 14943 is already open for ServerProtect access.

Remotely Deploying a Kernel Hook Module

You can use RemoteInstall to remotely deploy the KHM to multiple computers.

To deploy a KHM using RemoteInstall:

1. Download the latest KHM from the Trend Micro kernel support Web site:

   `http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=111&regs=NABU&lang_loc=1`

2. Copy the KHM to its corresponding directory on the deploying server.
3. Run RemoteInstall.

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

Verifying the Installation

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

To verify that ServerProtect is running properly:

1. Type the following command in command line:

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

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

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

Uninstalling ServerProtect

In order to remove ServerProtect, you must be logged on as *root*. In a terminal window, type `rpm -e SProtectLinux` to stop the ServerProtect service and remove the application.

Chapter 3

Post Installation Configuration

This chapter describes how to access the ServerProtect Web console and the configuration tasks after installation. Topics discussed include the following:

- *Logging On to the ServerProtect Web Console* on page 3-2
- *Setting Up an Administrator Password* on page 3-3
- *Configuring Proxy Server Settings* on page 3-4
- *Registering ServerProtect* on page 3-7
- *Activating ServerProtect* on page 3-8
- *Upgrading to the Full Version* on page 3-9
- *Updating Components* on page 3-12
- *Testing ServerProtect with the EICAR Test Virus* on page 3-12
- *Configuring rsyslog* on page 3-13

Logging On to the ServerProtect Web Console

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

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

The Logon screen displays in your browser window.

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

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

FIGURE 3-3. ServerProtect Web console Logon screen

The **Summary** screen displays. This screen is the default view when the Web console opens. If you have not registered and activated ServerProtect, the screen displays that the product has not been activated yet.

Make selections from the left menu to navigate the user interface.

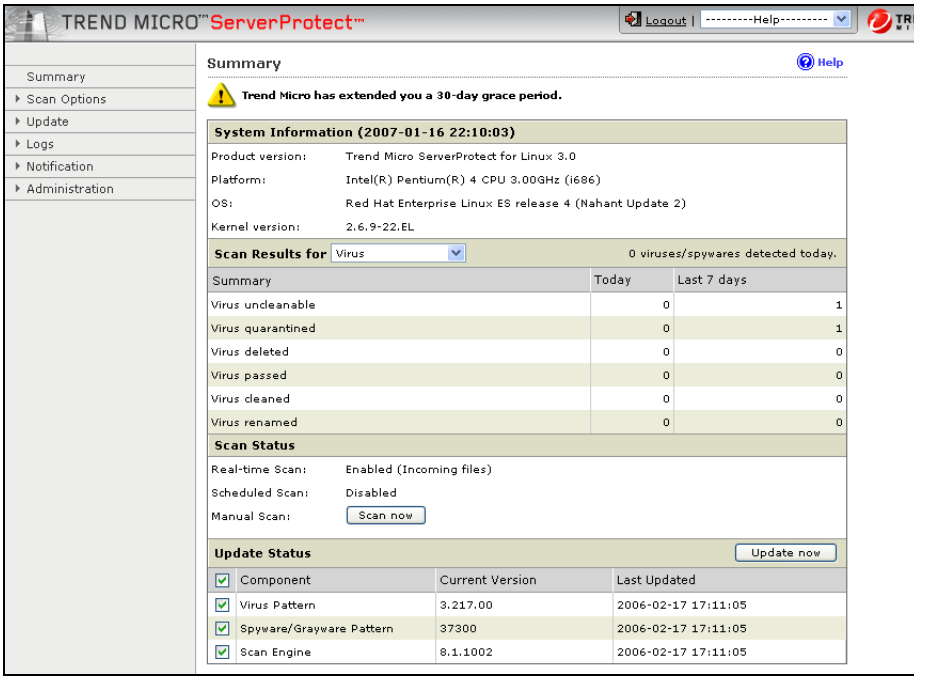

FIGURE 3-4. Default view of the Web console after login

Note: Real-time scanning is enabled by default.
Trend Micro recommends you set up your administrator account with a password, before you log off from the ServerProtect Web console.

Setting Up an Administrator Password

Click **Administrator** > **Password** in the left menu to display the Password screen. ServerProtect prompts you to supply your current password and your new password and to confirm your new password. Passwords must not exceed 32 characters, and should contain alphanumeric characters (A-Z, a-z, 0-9) and hyphens (-).

After the first logon, leave the **Current password** field blank and type the same information in **New password** and **Confirm password** fields. However, you can change your password at a later time on this screen. See *Setting Up an Administrator Password* on page 3-3 for more information.

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

For information on how to reset the password from the command line, see the description of the `-f` option for the `splxmain` command in the Administrator's Guide.

Configuring Proxy Server Settings

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

- License update
- Component update

General Proxy Settings

Follow the procedure below to configure proxy settings for License update features.

To configure proxy settings for License update:

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

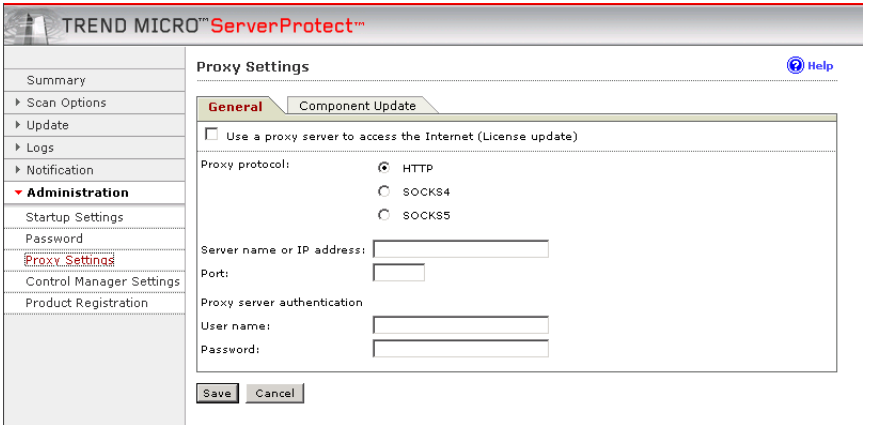

FIGURE 3-5. Proxy Settings General screen

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

Component Update Proxy Settings

Follow the procedure below to configure a proxy server for updating scan engine and pattern files.

To configure proxy settings for component update:

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

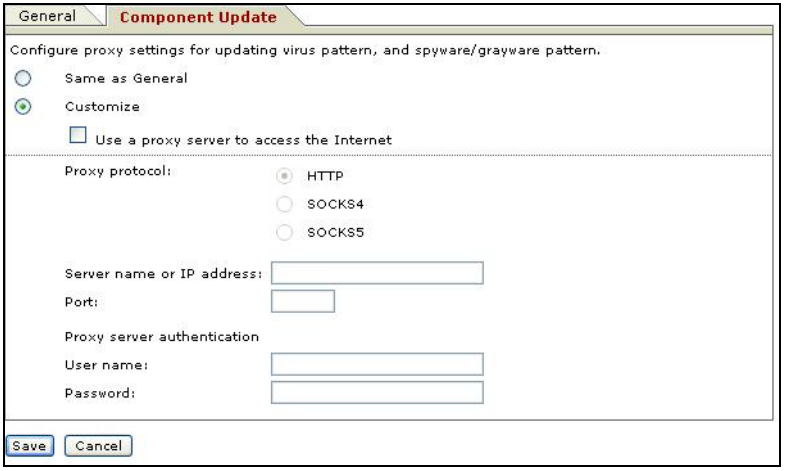

FIGURE 3-6. Proxy Settings Component Update screen

2. Select **Same as General** to use the same proxy server setting you configure in the General screen.
   - Select **Customize** to configure the proxy settings.
   - Select **Use proxy server to access the Internet** if you want to use a proxy server for component update. Then continue to Step i.

     Clear the **Use proxy server to access the Internet** check box if you do not want to use a proxy server for component updates. For example if the update server is located within your company network. Then skip to Step 3.

     i. Select **HTTP**, **SOCKS4,** or **SOCKS5** in the **Proxy protocol** field.

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

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

     iv. If you are using an optional proxy authentication user ID and password, type this information in the **User name** and **Password** fields.
3. Click **Save**.

Registering ServerProtect

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

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

Registration Key Format

A Registration Key displays in the following format:

`XX-XXXX-XXXX-XXXX-XXXX`

Activation Code (Serial Number) Format

An activate code (also referred to as serial number) displays in the following format:

`XX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`

Note: Some resellers may have already registered ServerProtect for you and given you the product Activation Code directly.
If you already have a ServerProtect Activation Code, follow the instructions in *Activating ServerProtect* on page 3-8 to activate ServerProtect.

To register your software using your Registration Key:

1. First, verify that you have received a Registration Key for ServerProtect. If you have not, contact your reseller.
2. On the ServerProtect Web console, click **Administration** > **Product Registration** on the left menu. The **Product Registration** screen displays.

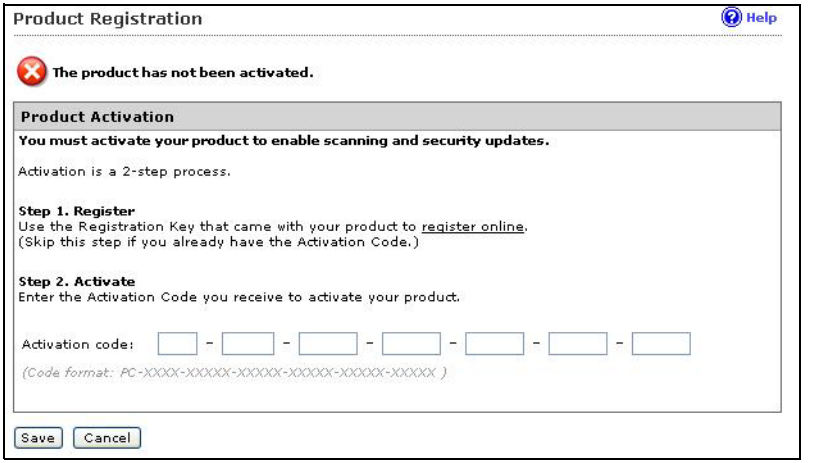

FIGURE 3-7. Proxy Settings Component Update screen

3. Click the register online link.
4. Follow the onscreen instructions to obtain the registeration key. Contact your Trend Micro representative for further details.

Activating ServerProtect

You can activate ServerProtect in one of the following ways:

- During the installation process
- Using the Product Registration screen in the Web console
- Type the following command in the `/opt/TrendMicro/SProtectLinux/SPLX.vsapiapp` folder:

  ```
  ./splxmain -q
  ```

Trend Micro recommends that you activate ServerProtect during installation. Refer to *Activating ServerProtect* on page 3-8 for more information.

To activate ServerProtect in the Product Registration screen:

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

To activate ServerProtect at the command prompt:

1. Navigate to the following directory:

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

2. Issue the following command to activate ServerProtect:

   ```
   ./splxmain -q <Activation Code>
   ```

Upgrading to the Full Version

If you skip the registration/activation step during installation (by typing **Ctrl**+**D**), most product features (such as virus/spyware scan, component updates, etc.) will be inactive. You can view the status of your installed product (whether activated or not) in the **Product Registration** screen. The following screen example indicates that the product has not been activated.

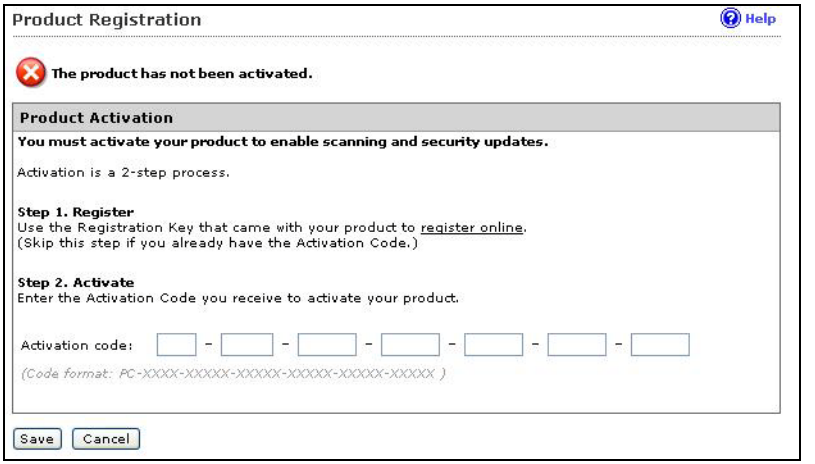

FIGURE 3-8. Product Registration screen: Inactive

If you are given an Activation Code that enables all ServerProtect features for a trial period, the **Product Registration** screen displays **Trial** in the **Version** field. The following shows an example screen.

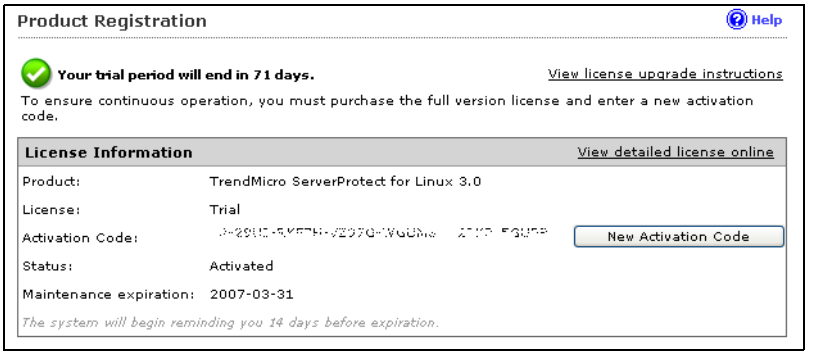

FIGURE 3-9. Product Registration screen: Trail Version

To upgrade ServerProtect to the full, licensed version, register and activate the product. Use the Registration Key included in the ServerProtect package or purchase one from your Trend Micro reseller to obtain an Activation Code (also known as a serial number) from Trend Micro Online Registration as described in *Registering ServerProtect* starting on

page 3-7.

The following screen indicates that your ServerProtect is a full, licensed version.

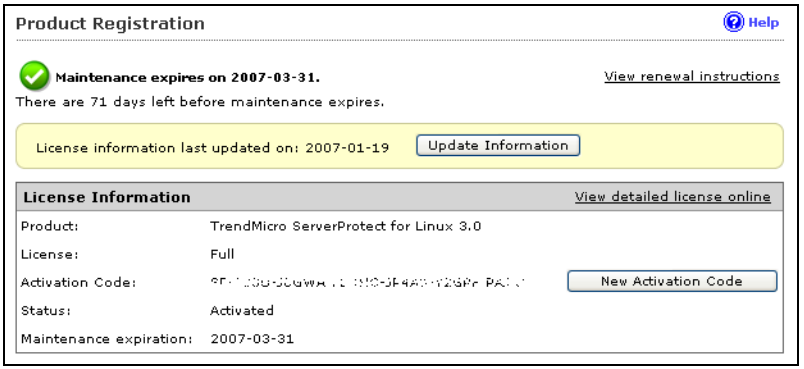

FIGURE 3-10. Product Registration screen: Full Version

Updating Components

Perform manual or scheduled virus pattern, spyware pattern and scan engine file updates to ensure up-to-date virus/malware or spyware protection.

To update components:

1. Display the Manual Update (click **Update > Manual Update**) or Scheduled Update screen (click **Update > Scheduled Update**).
2. Select the **Component** check box.
3. Click **Save**.

Initiating Automatic Update on Control Manager

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

To initiate automatic update from Control Manager:

1. Make sure you have successfully registered ServerProtect to Control Manager.
2. Log onto the Control Manager Web console and select **Product Programs** in the **Manual Download** or **Scheduled Download** screen.
3. From Control Manager, perform a component update.

Refer to the Administrator's Guide or the Trend Micro Control Manager Administrator's Guide for more information about managing products in Control Manager.

Testing ServerProtect with the EICAR Test Virus

After installing ServerProtect, verify that the application is running properly.

The European Institute for Computer Antivirus Research (EICAR) has developed a test virus to test your antivirus software. This script is an inert text file. The binary pattern is included in the virus pattern file from most antivirus vendors.

The test virus is not a virus and does not contain any program code; it will cause no harm and it will not replicate.

WARNING! **Never use real viruses to test your antivirus installation.**

Obtaining the EICAR Test File

You can download the EICAR test file from the following Web site:

`http://www.eicar.org/anti_virus_test_file.htm`

Alternatively, you can create your own EICAR test file by typing or copying the following characters into a text file, and then save the file with a `com` extension (for example, `virus.com`):

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

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.

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

Configuring rsyslog

To allow ServerProtect to store debug log information on Linux server configure rsyslog as follows:

1. Open `/etc/rsyslog.conf` and do the following:
   a. Add the following lines to the file:

      ```
      # this is for splx debug log
      local3.* /var/log/splx_usr.log
      ```

   b. For CentOS Linux 8 and Red Hat Enterprise Linux 8, search for **#module (load ="imklog")** and delete the character # from the text.

   c. Add the following lines to the file:

      ```
      # this is for KHM debug log
      ```

```
if $msg contains "SPLXMOD" and not($msg contains
"systemd-journal") then {
   action(type="omfile" file="/var/log/splx_kern.log")
}
```

2. Restart the rsyslog daemon by typing **service rsyslog restart** in the terminal.
3. Set the debug parameter (UserDebugLevel) in the tmsplx.xml file to 5.
4. Set the debug parameter (KernelDebugLevel) in the tmsplx.xml file to 3.
5. Restart ServerProtect by typing service splx restart.

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

Appendix A

Building and Installing Kernel Hook Module

This appendix shows you how to build and install Kernel Hook Module on RedHat. This appendix contains the following sections:

- *Introduction* on page A-2
- *Requirement* on page A-2
- *Installation* on page A-3

Introduction

Kernel Hook Module (KHM) is a kernel module for ServerProtect and it supports the real-time scan feature. You can use the same general procedure for building a kernel module to build the KHM on your Linux system. Command line examples are provided in this document.

The following is an overview of the process:

Step 1. Determine your Linux kernel version and architecture

Step 2. Prepare the kernel source

Step 3. Configure the kernel source

Step 4. Build the KHM

Step 5. Test the KHM

Step 6. Install the KHM

Step 7. Restart ServerProtect

Requirement

To build the KHM successfully, you need the following:

- root access to the Linux system
- GCC
- GNU Make
- the corresponding kernel source and configuration file for your running kernel
- elfutils-libelf-devel

Installation

Step 1. Determine your Linux kernel version and architecture

Use the following command to determine the kernel version of your Linux system:

```
uname -r
```

This command returns a string (for example, "4.18.0-80.el8"). In this document, replace "`<Kernel Version>`" with this string.

Use the following command to determine the kernel architecture of your Linux system:

```
uname -m
```

This command returns a string (typically, "`x86_64`"). In this document, replace "`<Arch>`" with this string.

Note: You can also obtain the same information on the Summary screen in the ServerProtect Web console.

Step 2. Prepare the kernel source

Make sure the configured kernel source is available on your Linux system. This section describes how to prepare the kernel source for the following Linux systems:

- Red Hat Enterprise Linux 8
- SUSE Linux Enterprise Server 15
- CentOS Linux 8
- A Linux system you custom build

To determine which distribution you are using, check the Summary screen in the ServerProtect Web console or by typing the following command:

```
uname -a
```

For Red Hat Enterprise Linux 8 and CentOS 8:

Make sure you have installed the following RPM package:

- kernel-devel
- kernel

Note: To check if you have already installed one of these packages, see #1 in Troubleshooting for more information.

Type the following command to install the RPM package. The package you choose to install depends on your running kernel version.

```
rpm -ivh <rpm package name>
```

Example:

If your running kernel version is "4.18.0-80.el8" and the kernel architecture is "x86_64", type the following:

```
rpm -ivh kernel-devel-4.18.0-80.el8.x86_64.rpm
```

In addition to using the command line, you can use one of the following methods to install the packages:

- Linux desktop environment (for example in GNOME, click **Application > System Settings > Add/Remove Program**).
- the **up2date** program

For SUSE Linux Enterprise Server 15:

Make sure you have installed the following RPM packages on your Linux system:

- kernel-source
- kernel-syms
- kernel-default
- .kernel-default-devel
- .kernel-macros
- .kernel-devel

Note: To check if you have already installed one of these packages, see troubleshooting solution 1 in *Building and Installing KHM* on page B-2 for more information.

Type the following command to install the packages:

```
rpm -ivh <rpm package name>
```

Example:

If your running kernel version is "4.12.14-195-default", type the following commands:

```
rpm -ivh kernel-source-4.12.14-195.1.noarch.rpm
```

```
rpm -ivh kernel-syms-4.12.14-195.1.x86_64.rpm
```

```
rpm -ivh kernel-default-devel-4.12.14-195.1.x86_64
```

```
rpm -ivh kernel-macros-4.12.14-195.1.noarch
```

```
rpm -ivh kernel-macros-4.12.14-195.1.noarch
```

```
rpm -ivh kernel-default-4.12.14-195.1.x86_64
```

In addition to using the command line, you can also use the YaST tool to install the packages.

For the customized kernel you built yourself

Make sure the kernel source is configured and prepared correctly with your running kernel version.

Generally, you can do this by copying the configuration files from the `/boot` directory to the kernel source directory (eg. `/usr/src/linux-<Kernel Version>`) and type the `make oldconfig`" and `make modules_prepare` commands:

```
cp /boot/config-<Kernel Version> /usr/src/linux-<Kernel Version>/.config
```

```
cd /usr/src/linux-<Kernel Version>
```

```
make oldconfig
```

```
make modules_prepare
```

Step 3. Configure the kernel source

In order to reduce the size of the compiled KHM, Trend Micro recommends not selecting the **Compile the kernel with debug info** option in the **Kernel Hacking** menu for kernel configuration.

You can find your kernel source in the following directory:

```
cd /lib/modules/<Kernel Version>/build
```

Then, type the following command in your kernel source directory to display the configuration UI.

```
make menuconfig
```

In the **Kernel Hacking** menu, locate **Compile the kernel with debug info**. If an asterisk appears before this item, press "N" on the keyboard to clear the asterisk. Then exit the configuration UI and save the settings.

WARNING! **Clear only the Compile the kernel with debug info option in the configuration UI. Do NOT change other options; otherwise you may encounter kernel panic while using the KHM.**

Note: If you experience problems using the "make menuconfig" command, the "ncurses" package may not be installed in your Linux system. Do one of the following:
- Install the package: you can obtain the package from the Linux installation CD or download it from your Linux vendor's web site.
- Modify the `.config` file in the kernel source directory: change `CONFIG_DEBUG_INFO=y` to `CONFIG_DEBUG_INFO=n` in the file.

After the configuration, type the following command to prepare the source for kernel module compilation:

```
make modules_prepare
```

Step 4. Build the KHM

Note: For x86_64 architecture, if the build process is not successful, see #6 in Troubleshooting for more information.

Go to the directory where the KHM source is located (the default location is `/opt/TrendMicro/SProtectLinux/SPLX.module/src/module`).

Use the `make` command to generate a new KHM.

```
cd /opt/TrendMicro/SProtectLinux/SPLX.module/src/module
make
```

You can ignore the warning messages during the build process. If the build process is successful, a KHM with the file name `splxmod-<Kernel Version>.<Arch>.o` will be generated in the `bin` directory.

Step 5. Test the KHM

Note: Trend Micro recommends performing this KHM test before installing it to your computer. This prevents you from installing a non-working KHM in your Linux computer, causing the computer to hang after every system reboot.

Before you perform the KHM test, stop the ServerProtect services.

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

Type the following command to perform a basic functional test for the KHM you have just built. This test should take less than 5 seconds. If the test takes longer than 5 seconds, this indicates that your system has stopped responding.

```
make test
```

WARNING! This test script will only perform basic tests to ensure that the KHM MAY work. A successful test result does NOT guarantee that the KHM can work properly under all circumstances. During the KHM test, your system may hang or you may experience a kernel panic. Trend Micro recommends performing this operation on a test computer.

Refer to #5 in Troubleshooting for more information if:

- your Linux computer stops responding during the KHM test
- the KHM fails the test (in this case, do not install the KHM)

Step 6. Install the KHM

If the compiled KHM passed the test successfully, you can install it by typing the install script:

```
make install
```

This will copy the compiled KHM into the `/opt/TrendMicro/SProtectLinux/SPLX.module` directory. If there is already a KHM with the same name in that directory, the original file will automatically be renamed with a `.bak` suffix.

If your Linux computer stops responding after a system reboot, see #8 in Troubleshooting for more information.

Step 7. Restart ServerProtect

Restart ServerProtect to use the newly installed KHM:

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

Appendix B

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* on page B-2
- *Before Contacting Technical Support* on page B-4
- *Contacting Technical Support* on page B-5
- *About TrendLabs* on page B-6
- *Other Useful Resources* on page B-8
- *About Trend Micro* on page B-9

Troubleshooting

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

Problem with Missing Dependent Libraries in Linux

To install ServerProtect successfully on your Linux computer, make sure the following dependent libraries are installed.

- glibc
- libgcc
- zlib
- bzip2
- libuuid
- libstdc++ (Red Hat and CentOS only)
- nss-softokn-freebl (Red Hat and CentOS only)
- perl-Sys-Syslog (Red Hat and CentOS only)

Building and Installing KHM

1. What should I do if the `make` program prompts me to install the kernel source package or kernel object package?

   Make sure you have completed *Step 2. Prepare the kernel source* on page A-3 correctly. To check if the required RPM packages are already installed, type the following command:

   ```
   rpm -q <rpm package name>
   ```

   If a required package is not installed, obtain the package from your Linux vendor's website or the installation source (such as CD-ROMs) and install it.

2. I am using a kernel which is custom-built and I have the kernel source, but the "`Unable to locate source package`" message still displays after I typed the "make" command.

   You can try copying your kernel source or creating symbolic links to the `/usr/src/linux-<Kernel Version>` directory and try the `make` command again.

3. The test program displays a "`Cannot find ... symbol in System.map`" message.

   For the KHM to work properly, it must obtain certain symbol addresses from `/boot/System.map-<Kernel Version>`. If this file is not found, the KHM will not work properly. If the file does not exist, you may need to rebuild your Linux kernel to get this file.

4. What should I do if the KHM build process failed?

   First, visit the Trend Micro website to see if the KHM for your Linux system is available. If so, download the KHM to use it.

   You can check if Trend Micro has updated the KHM source code on the Trend Micro website. Since the Linux kernel is updated regularly, Trend Micro will also update the KHM source code for it to work with the new Linux kernel.

   Since the KHM code is published under GPL, you can also try to fix the problem yourself by modifying the source code.

5. What should I do if the test program crashes/hangs or if the "`Cannot remove KHM from kernel`" message displays?

   First, reboot your system and then visit the Trend Micro website to see if the KHM for your Linux system is available. If so, just download the KHM to use it.

   You can check if Trend Micro has updated the KHM source code on the Trend Micro website. Since the Linux kernel is updated regularly, Trend Micro will also update the KHM source code for it to work with the new Linux kernel.

   Since the KHM code is published under GPL, you can also try to fix the problem yourself by modifying the source code.

6. After installing the KHM, the Linux computer hangs after a system reboot.

   This problem may be caused by the installed KHM that you have not tested to verify whether it can run properly in your Linux computer Follow the steps below to solve this problem:

   a. Reboot your Linux computer and enter the "`init 1`" mode (you can do this by changing the kernel boot up parameter in the boot loader, such as GRUB).

   b. Type the following command to remove the KHM in the `/opt/TrendMicro/SProtectLinux/SPLX.module` directory:

      ```
      rm
      /opt/TrendMicro/SProtectLinux/SPLX.module/splxmod-‘uname
      -r‘. ‘uname -m‘.o
      ```

c. Reboot your computer again. The Linux system should start without any problems. However, since there is no KHM installed, ServerProtect real-time scan is not enabled. To enable real-time scan, build the KHM again.

To avoid this problem, Trend Micro recommends you perform "make test" before installing the newly built KHM.

Default Password

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

Web Console Rejects Passwords

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

- **Incorrect password—**Passwords are case-sensitive. For example, "TREND" is different from "Trend" or "trend."
- **ServerProtect's customized Apache server does not respond—**Check `splxhttpd` status. For additional information, see the Administrator's Guide.

Debug Logs

Refer to the Administrator's Guide for more information on debug logging. ServerProtect provides the following debug options:

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

Before Contacting Technical Support

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

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

  To search the Knowledge Base, visit

  `http://esupport.trendmicro.com`

Contacting Technical Support

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

Email support

`support@trendmicro.com`

Help database—configuring the product and parameter-specific tips

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

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

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

Product updates and patches

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

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

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

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

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

About TrendLabs

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus/malware outbreaks and provide urgent support.

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.

About Software Updates

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

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

- **Hot fix—**A hot fix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes don't (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).
- **Critical Patch—**A critical patch is a hot fix focusing on critical issues that is suitable for deployment to all customers. Windows critical patches include a Setup program, while non-Windows patches commonly have a setup script.

- **Patch—**A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Service Pack—**A service pack is a consolidation of hot fixes, patches, and feature enhancements significant enough to be considered a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

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

`http://esupport.trendmicro.com`

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

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

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

Known Issues

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

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

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

`http://esupport.trendmicro.com`

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

Other Useful Resources

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

Internet-based tools and services include:

- Virus Map— monitor virus/malware incidents around the world
- Virus risk assessment— the Trend Micro online virus/malware protection assessment program for corporate networks.

About Trend Micro

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

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

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

`http://www.trendmicro.com`

Index

Symbols

1-2—1-4, 2-3—2-4, 2-6, 2-8—2-10, 2-12—2-14, 2-16—2-19, 3-2—3-4, 3-7—3-9, 3-12—3-13
`/etc/init.d/splx status` 2-19

A

Accessing the Web console 2-17, 3-2
Activate the product 2-7
Activating the product 3-9
Activation Code 1-4, 3-7
Administrator password
  Resetting 3-4
  Setting 3-3
Audience P-2

C

Component update 3-12
Configuration file 2-8
  ConfigFilePath 2-10
  group deploy 2-13
  RemoteInstall tool directories and files 2-9
Control Manager
  Folder name 2-6
  Product display name 2-6
  Proxy setting 2-6
  Server IP address 2-6
  Server port 2-6

D

Default password B-4
Document conventions P-3
Documentation set P-2

E

End user license agreement 2-4
European Institute of Computer Antivirus Research (EICAR) 3-12

H

Hardware requirements 1-2
  CPU 1-2
  Disk space 1-2
  Memory 1-2
Hot fix B-6

I

Installation 2-1
  Verifying 2-19
Installation method 1-4
    Local installation 2-3
  Remote 2-8

K

Kernel Hook Module 2-16
  Extracting package 2-17
  Installation 2-17
Kernel Hook Module (KHM) 2-16
`KHM.module/` 2-9
Knowledge Base P-2, B-5, B-7
Known issues B-7
  URL for Knowledge Base describing B-7
  URL for readme documents describing B-7

L

Logon session control 3-2

M

Man pages P-2

O

Online help P-2

P

Password
  default B-4
  incorrect B-4

rejected B-4
Patch B-7
Patent No. 1-ii
Preface P-1
Pre-installation
Information you may need 1-3
Pre-installation steps 1-1
Product license 2-7
Proxy servers 1-3
Proxy setting 3-4
Component update 3-5
General 3-4

R

Readme file P-2
Real-time
scan 3-3
Register to Control Manager 2-5
Registration
Product 3-8
Registration key 3-7
Remote installation
Default configuration file 2-10
Deploy the KHM 2-18
Group deployment 2-13
Single deployment 2-12
Specify clients 2-11
`remote.install.splx` 2-9
RemoteInstall
conf keys 2-10
Convert CVS-formatted files 2-10
Extracting 2-9
Features 2-8
group deploy 2-13
Options 2-15
parameters 2-15
Result files after execution 2-14
Running 2-14
Subdirectory 2-9
`RemoteInstall` 2-9
RemoteInstall.conf
keys 2-10
`RemoteInstall.conf` 2-9—2-10
`RemoteInstall.csv` 2-9

S

ServerProtect 2-17
Service pack B-7
Skip product activation 2-8
Software requirements 1-2
Supported distributions and kernels 1-2
Supported Web browsers 1-3
Software updates B-6
hot fix B-6
patch B-7
service pack B-7
Start services 2-17
Starting ServerProtect services 2-17
`syslog-ng` 3-13
System requirements 1-2
Hardware 1-2
Software 1-2

T

Test virus 3-12
`tmsplx.xml` 2-9
`tmsplx.xml.template` 2-9
Trend Micro Control Manager 1-3
TrendLabs B-6
Troubleshooting B-2

U

Uninstallation 2-19
Update Center P-2
Upgrading to the full version 3-9
URLs
Knowledge Base containing known issues B-7
readme documents containing known issues B-7

V

virus doctors B-6

W

Web console
    password rejected B-4

X

`xmldeployer` 2-9
`xmlvalidator` 2-9

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: SPEM38858/191118