



3.2 TREND MICRO™ Smart Protection Server

Installation Guide

Security Made Smarter



Endpoint Security



Messaging Security



Protected Cloud



Web Security

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

<http://docs.trendmicro.com/en-us/enterprise/smart-protection-server.aspx>

Trend Micro, the Trend Micro t-ball logo, TrendLabs, OfficeScan, and Smart Protection Network 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 © 2017. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM37757/170322

Release Date: April 2017

Protected by U.S. Patent No.: Patents pending.

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

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

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Table of Contents

Preface

Preface	iii
About Trend Micro	iv
Product Documentation	iv
Audience	iv
Document Conventions	v

Chapter 1: Planning Smart Protection Server Installation and Upgrade

System Requirements	1-2
Planning for Deployment	1-5
Best Practices	1-5
Deployment Guidelines	1-6
Preparing to Install	1-6

Chapter 2: Installing Smart Protection Server

Performing a Fresh Installation	2-2
Installing Smart Protection Server	2-2

Chapter 3: Post-Installation Tasks

Post-Installation	3-2
Initial Configuration	3-2

Chapter 4: Technical Support

Troubleshooting Resources	4-2
Using the Support Portal	4-2
Threat Encyclopedia	4-2

- Contacting Trend Micro 4-3
 - Speeding Up the Support Call 4-4
- Sending Suspicious Content to Trend Micro 4-4
 - Email Reputation Services 4-4
 - File Reputation Services 4-5
 - Web Reputation Services 4-5
- Other Resources 4-5
 - Download Center 4-5
 - Documentation Feedback 4-6

Appendix A: Migration Settings

- Migrating Settings Prerequisites A-2
- Migrating Settings from Smart Protection Server 3.x A-3

Index

- Index IN-1

Preface

Preface

Welcome to the Smart Protection Server™ Installation and Upgrade Guide. This document contains information about product settings.

Topics include:

- *About Trend Micro™ on page iv*
- *Product Documentation on page iv*
- *Audience on page iv*
- *Document Conventions on page v*

About Trend Micro™

Trend Micro provides virus protection, antispyware, and content-filtering security software and services. Trend Micro helps customers worldwide stop malicious code from harming their computers.

Product Documentation

The Smart Protection Server documentation consists of the following:

DOCUMENTATION	DESCRIPTION
Installation and Upgrade Guide	Helps you plan for installation, upgrades, and deployment.
Administrator's Guide	Helps you configure all product settings.
Online Help	Provides detailed instructions on each field and how to configure all features through the user interface.
Readme file	Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The documentation is available at:

<http://downloadcenter.trendmicro.com/>

Audience




The Smart Protection Server documentation is written for IT managers and administrators. The documentation assumes that the reader has in-depth knowledge of computer networks.

The documentation does not assume the reader has any knowledge of virus/malware prevention or spam prevention technology.

Document Conventions

The Smart Protection Server User's Guide uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 WARNING!	Critical actions and configuration options

Chapter 1

Planning Smart Protection Server Installation and Upgrade

This chapter includes information about planning for a fresh installation or upgrade of Smart Protection Server.



Topics include:



- *System Requirements on page 1-2*
- *Planning for Deployment on page 1-5*
- *Preparing to Install on page 1-6*


System Requirements

The following table lists the system requirements:

TABLE 1-1. System Requirements

HARDWARE/ SOFTWARE	REQUIREMENTS
Hardware	<ul style="list-style-type: none">• 2.0GHz Intel™ Core2 Duo™ 64-bit processor supporting Intel™ Virtualization Technology™ or equivalent• 2GB of RAM (Trend Micro recommends 4GB)• 50 GB disk space when installed on a virtual machine <hr/> <div data-bbox="420 646 467 686"></div> <div data-bbox="477 646 530 667">Note</div> <div data-bbox="477 683 1091 735">Smart Protection Server automatically partitions the detected disk space as required.</div> <hr/> <div data-bbox="420 792 467 833"></div> <div data-bbox="477 792 530 813">Note</div> <div data-bbox="477 829 1063 963">The Blocked URLs stop collecting data if Smart Protection Server detects that the available disk space is less than 1GB. Smart Protection Server starts collecting data again once the administrator has made at least 1.5GB of disk space available.</div> <hr/> <ul style="list-style-type: none">• Monitor with 1024 x 768 or greater resolution with 256 colors or higher

HARDWARE/ SOFTWARE	REQUIREMENTS
Virtualization	<ul style="list-style-type: none">• Microsoft™ Windows Server™ 2008 R2 Hyper-V™• Microsoft™ Windows Server™ 2012 Hyper-V™• Microsoft™ Windows Server™ 2012 R2 Hyper-V™• Microsoft™ Windows Server™ 2016 Hyper-V™• VMware™ ESXi™ Server 6.5, 6.0 Update 2, 5.5 Update 3b• Citrix™ XenServer™ 7.1, 7.0, 6.5 <hr/> <div data-bbox="516 574 561 613"></div> <div data-bbox="575 574 626 597">Note</div> <div data-bbox="575 613 1099 662">If you use a Citrix™ XenServer, create a new Virtual Machine using the Other install media template.</div> <hr/> <div data-bbox="516 724 561 763"></div> <div data-bbox="575 724 626 747">Note</div> <div data-bbox="575 763 1184 812">Smart Protection Server already has a purpose-built, hardened, performance-tuned 64-bit Linux operating system.</div>

HARDWARE/ SOFTWARE	REQUIREMENTS
Virtual Machine	<ul style="list-style-type: none">• CentOS 7 64-bit or CentOS 64-bit• Allocate at least 2GB of RAM to the Virtual Machine. Trend Micro recommends you allocate 4GB.• 2.0GHz processor• 2 virtual processors minimum (4 virtual processors recommended)• 50 GB disk space• 1 network device• Network Device <hr/> <div> Note<p>The Smart Protection Server kernel module will install the VMWare Tools module vmxnet3. This means that VMWare Tools do not need to be installed after installing Smart Protection Server.</p><p>If you choose a vmxnet3 NIC during installation, the message Minimum hardware requirements were not met might appear because the vmxnet3 driver has not been installed at that point. This message can be ignored and the installation will proceed normally.</p></div> <hr/>
Web Console	<ul style="list-style-type: none">• Microsoft Edge™• Microsoft™ Internet Explorer™ 11• Mozilla™ Firefox™ 3.6.0 or later• Adobe™ Flash™ Player 8.0 or above is required for viewing graphs in widgets• 1024 x 768 or greater resolution with 256 colors or higher

Planning for Deployment

The following section provides information on how to determine the type of environment to configure when installing local Smart Protection Server computers.

Best Practices

- Avoid performing Manual scans and Scheduled scans simultaneously. Stagger the scans in groups.
- Avoid configuring all endpoints from performing Scan Now simultaneously. For example, the **Perform scan now after update** option.
- Install multiple Smart Protection Server computers to ensure the continuity of protection in the event that connection to a Smart Protection Server is unavailable.
- Customize Smart Protection Server for slower network connections, about 512Kbps, by making changes to the `ptngrowth.ini` file.

Configuring the `ptngrowth.ini` File

Procedure

1. Open the `ptngrowth.ini` file in `/var/tmcss/conf/`.
2. Modify the `ptngrowth.ini` file using the recommended values below:

```
[COOLDOWN]
ENABLE=1
MAX_UPDATE_CONNECTION=1
UPDATE_WAIT_SECOND=360
```

3. Save the `ptngrowth.ini` file.
4. Restart the `lighttpd` service by typing the following command from the Command Line Interface (CLI):

```
systemctl restart lighttpd
```

Deployment Guidelines

Consider the following when setting up your local Smart Protection Server:

- Smart Protection Server is a CPU-bound application. This means that increasing CPU resources increases the number of simultaneous requests handled.
- Network bandwidth may become a bottleneck depending on network infrastructure and the number of simultaneous update requests or connections.
- Additional memory might be required if there is a large number of concurrent connections between Smart Protection Server computers and endpoints.

Preparing to Install

The Smart Protection Server installation process formats your existing system for program installation. VMware or Hyper-V installation requires the creation of a virtual machine before installation. After determining the number of Smart Protection Server computers to use for your network, you can begin the installation process.



Tip

Install multiple Smart Protection Server computers to ensure the continuity of protection in the event that connection to a Smart Protection Server is unavailable.

You need the following information for the installation:

- Proxy server information
- A virtual machine server that fulfills the requirements for your network

Chapter 2

Installing Smart Protection Server

This chapter includes information about upgrading and installing Smart Protection Server.

Topics include:

- *Performing a Fresh Installation on page 2-2*

Performing a Fresh Installation

After preparing the requirements for installation, run the installation program to begin installation.

Installing Smart Protection Server

This page describes the process for installing Smart Protection Server.

**Note**

For users of Smart Protection Server 3.0 or 3.1, a command line Migration Tool allows you to transfer preconfigured settings to Smart Protection Server 3.2.

For a complete list of prerequisites required to begin migrating, see [Migrating Settings Prerequisites on page A-2](#).

Procedure

1. Create a virtual machine on your VMware or Hyper-V server and specify the virtual machine to boot from the Smart Protection Server ISO image.

**Note**

For more information, refer to the Virtual Machine section in [System Requirements on page 1-2](#).

2. Power on the virtual machine.

The **Welcome to Smart Protection Server** screen appears.



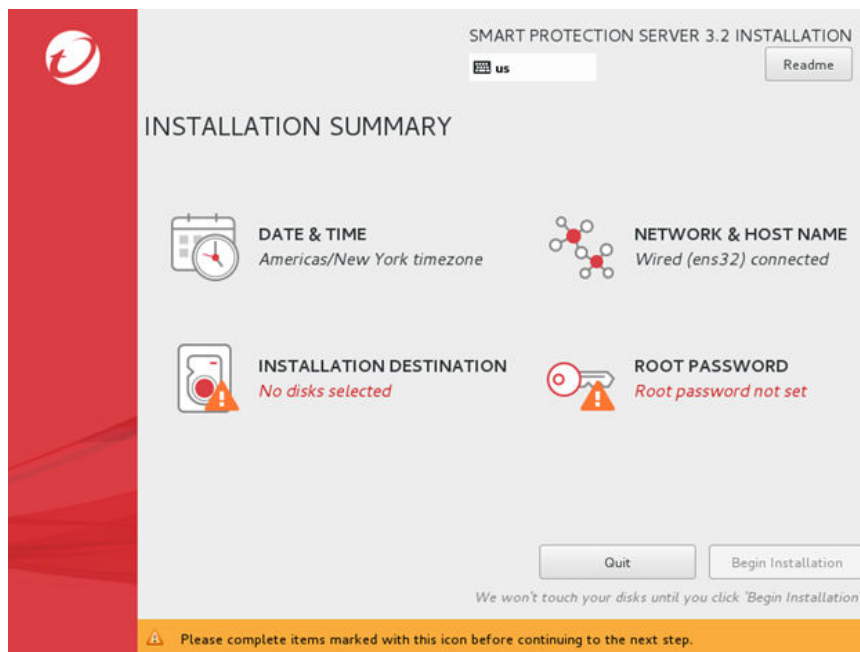
3. Select the language for this installation of Smart Protection Server.
4. Click **Continue**.

The **Trend Micro Smart Protection Server License Agreement** screen appears.



5. Click **Accept** to agree to the terms and conditions.

The **INSTALLATION SUMMARY** screen appears.



6. Click **DATE & TIME** to verify your date and time settings.
 - a. To synchronize date and time settings with your network, enable **Network Time**.
 - b. To customize the date and time, select your **Region** and **City** from the drop-down lists, or click your region on the map.
 - c. Click **Done**.
7. Click **NETWORK & HOST NAME** to verify your Network Adapter settings.

**Note**

To change the active on boot device after installation, log on to the Command Line Interface (CLI).

If there are multiple network devices, configure settings for all devices.

- a. If your environment requires advanced network settings, click **Configure....**

**Note**

The **Configure...** button allows you to configure IPv4 and IPv6 settings. The default setting for IPv4 is **Dynamic IP configuration (DHCP)**. The default setting for IPv6 is **Automatic neighbor discovery**.

- b. Click **Done**.
8. Click **INSTALLATION DESTINATION** to select the installation disk.
 - a. From the **Local Standard Disks** section, select a virtual disk.
 - b. Click **Done**.
 9. Click **ROOT PASSWORD** to create the following passwords:
 - **Root Password:** Creates a password for the root account.

The root account is used to gain access to the operating system shell and has all rights to the server. This account includes the most privileges.
 - **Admin Password:** Creates a password for the admin account.

The admin account is the default administration account used to access the Smart Protection Server web and CLI product consoles. This account includes all rights to the Smart Protection Server application, but does not include access rights to the operating system shell.

**Note**

Passwords must be a minimum of six characters and a maximum of 32 characters. To design a secure password, consider the following:

- Include both letters and numbers
- Avoid words found in any dictionary (of any language)
- Intentionally misspell words
- Use phrases or combine words
- Use a combination of uppercase and lowercase letters
- Use symbols

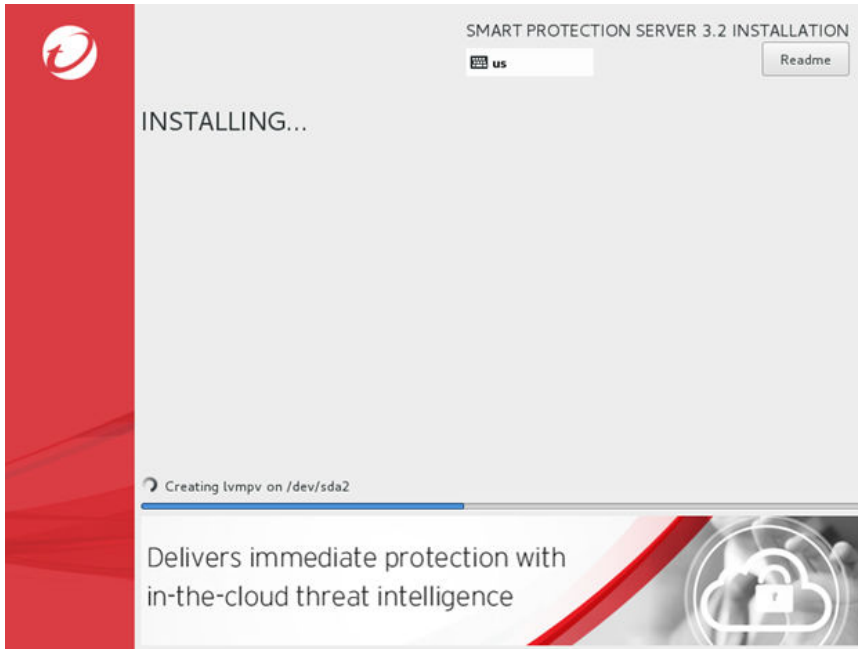
a. Click **Done**.

10. Click **Begin Installation**.

**WARNING!**

Continuing with the installation formats and partitions the necessary disk space and installs the operating system and application. If there is any data on the hard disk that cannot be erased, cancel the installation and back up the information before proceeding.

The installation begins. After the installation completes, the system restarts.

**Note**

You can obtain the installation log file in the following location:

`/root/install.log`

11. For users of Smart Protection Server 3.0 or 3.1, use the command line Migration Tool to transfer preconfigured settings to Smart Protection Server 3.2.

**Note**

For more information, see [*Migrating Settings from Smart Protection Server 3.x on page A-3*](#)

12. Log on to the Smart Protection Server web console to perform post installation tasks, such as configuring proxy settings. Log on to the Smart Protection Server

CLI shell if you need to perform additional configuration, troubleshooting or maintenance tasks.

**Note**

Use the **root** account to log on to the operating system shell with full privileges.

13. Perform post installation tasks.

**Note**

For more information, see *Post-Installation Tasks on page 3-1*.

Chapter 3

Post-Installation Tasks

This chapter includes information about Smart Protection Server post installation tasks.

Topics include:

- *Post-Installation on page 3-2*
- *Initial Configuration on page 3-2*

Post-Installation

Trend Micro recommends performing the following post-installation tasks:

- If you installed with minimum system requirements, disable the Blocked Web Access Log from the Command Line Interface (CLI) with your admin account by typing:

```
enable  
disable adhoc-query
```

- Perform initial configuration. See [Initial Configuration on page 3-2](#)
- Configure Smart Protection Server settings on other Trend Micro products that support smart scan solutions.



Note

The Real Time Status widget and Smart Protection Server CLI console display Smart Protection Server addresses.

VMWare Tools do not need to be installed after installing Smart Protection Server. The server kernel module contains the VMWare Tools module (vmxnet3) Smart Protection Server requires.

Initial Configuration

Perform the following tasks after installation.



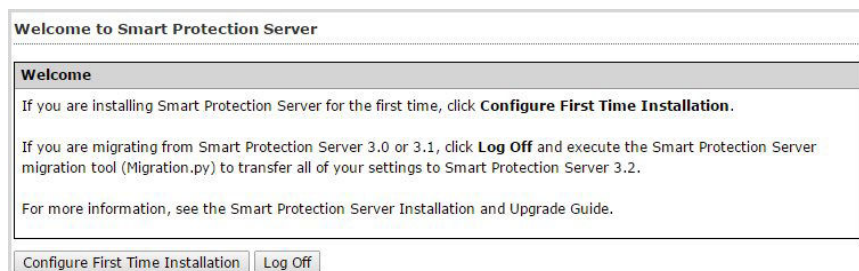
Important

If you are migrating from Smart Protection Server 3.0 or 3.1, execute the Smart Protection Server Migration Tool (Migration.py) to transfer all of your settings to Smart Protection Server 3.2 before continuing.

Procedure

1. Log on to the web console.

The **Welcome** screen appears.



2. Click **Configure First Time Installation**.

The first time installation wizard appears.

3. Select the **Enable File Reputation Service** check box to use File reputation.

Configuration Wizard for first time installation

[? Help](#)

Step 1:File Reputation Service >>> Step 2 >>> Step 3 >>> Step 4

File Reputation Service

☒ Enable File Reputation Service

Protocol	Server Address
HTTP, HTTPS	http:// IPv4 addr /tmcss
	http://[IPv6 addr]/tmcss
	http://localhost.localdomain/tmcss
	https:// IPv4 addr /tmcss
	https://[IPv6 addr]/tmcss
	https://localhost.localdomain/tmcss

>

- Click **Next**.

The Web Reputation Service screen appears.

- Select the **Enable Web Reputation Service** check box to enable Web Reputation.

Configuration Wizard for first time installation

Step 1 >>> **Step 2: Web Reputation Service** >>> Step 3 >>> Step 4

Web Reputation Service

☒ Enable Web Reputation Service

Protocol	Server Address
HTTP	http://[IP address of the Web Reputation Service]
	http://[IP address of the Web Reputation Service]
	http://[IP address of the Web Reputation Service]

Filter Priority

1. User-defined blocked URLs ▼
2. User-defined approved URLs
3. Web Blocking Pattern

< Back Next >


6. (Optional) The filter priority settings allow you to specify the filter order for URL queries.
7. Click **Next**.

The Smart Feedback screen appears.

Configuration Wizard for first time installation

Help

Step 1 >>> Step 2 >>> **Step 3: Smart Feedback** >>> Step 4



TREND MICRO™
SMART
PROTECTION
NETWORK

The Trend Micro Smart Protection Network is a next generation cloud-client content security infrastructure protection against the latest threats.
[Learn more](#)

Smart Feedback

When enabled, Trend Micro Smart Feedback shares anonymous threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. You can disable Smart Feedback anytime through this console.

☒ Enable Trend Micro Smart Feedback (recommended)

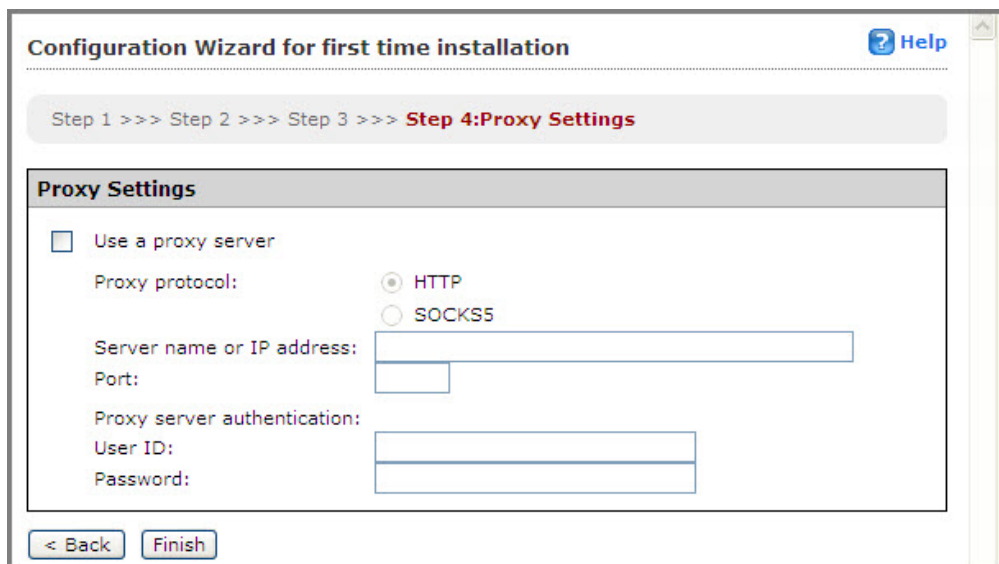
Your industry (optional):

< Back

Next >

8. Select to use Smart Feedback to help Trend Micro provide faster solutions for new threats.
9. Click **Next**.

The Proxy Settings screen appears.



The screenshot shows a web-based configuration wizard titled "Configuration Wizard for first time installation". At the top right is a "Help" link with a question mark icon. Below the title is a progress bar showing "Step 1 >>> Step 2 >>> Step 3 >>> Step 4: Proxy Settings", with "Step 4: Proxy Settings" highlighted in red. The main content area is titled "Proxy Settings" and contains the following options and input fields:

- ☐ Use a proxy server
- Proxy protocol:
 - ☒ HTTP
 - ☐ SOCKS5
- Server name or IP address:
- Port:
- Proxy server authentication:
 - User ID:
 - Password:

At the bottom of the form are two buttons: "< Back" and "Finish".

10. Specify proxy settings if your network uses a proxy server.
11. Click **Finish** to complete the initial configuration of Smart Protection Server.

The Summary screen of the web console displays.



Note

Smart Protection Server will automatically update pattern files after initial configuration.

Chapter 4

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 4-2*
- *Contacting Trend Micro on page 4-3*
- *Sending Suspicious Content to Trend Micro on page 4-4*
- *Other Resources on page 4-5*

Troubleshooting Resources

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

Using the Support Portal

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

Procedure

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



Tip

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

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

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

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <http://about-threats.trendmicro.com/us/threatencyclopedia#malware> to learn more about:

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

Contacting Trend Micro

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

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

<https://ers.trendmicro.com/>

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

<http://esupport.trendmicro.com/solution/en-US/1112106.aspx>

File Reputation Services

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

<http://esupport.trendmicro.com/solution/en-us/1059565.aspx>

Record the case number for tracking purposes.

Web Reputation Services

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

<http://global.sitesafety.trendmicro.com/>

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

Other Resources

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

Download Center

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

<http://www.trendmicro.com/download/>

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

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Appendix A

Migration Settings

This chapter includes information about using the Migration Tool to migrate settings from Smart Protection Server 3.x.

Topics include:

- *Migrating Settings Prerequisites on page A-2*
- *Migrating Settings from Smart Protection Server 3.x on page A-3*

Migrating Settings Prerequisites

Smart Protection Server provides a command line Migration Tool which allows you to transfer preconfigured settings from Smart Protection Server 3.0 or 3.1 to the latest version.

**Important**

You can only migrate settings from previous Smart Protection Server versions before you initialize the Smart Protection Server 3.2 computer. After initializing the Smart Protection Server 3.2 computer, you can no longer migrate settings unless you uninstall and reinstall the server.

The following prerequisites are required to begin migrating:

REQUIREMENT	DESCRIPTION
Virtual machine	<ul style="list-style-type: none">• Smart Protection Server 3.2 requires a virtual machine instance with at least the same specifications as the computer that you want to migrate settings from.• The Smart Protection Server 3.2 ISO must be installed on the virtual machine instance before running the tool.
SSH	<p>SSH must be enabled on the Smart Protection Server computer that you want to migrate settings from.</p> <p>For more information, see the Online Help or Administrator's Guide.</p>
Suspicious Object synchronization	<p>If Suspicious Objects synchronization is enabled, ensure that there is a working connection between the new virtual machine and the Suspicious Objects source.</p>

Migrating Settings from Smart Protection Server 3.x

Smart Protection Server provides a command line Migration Tool which allows you to transfer preconfigured settings from Smart Protection Server 3.0 or 3.1 to the latest version.



Important

You can only migrate settings from previous Smart Protection Server versions before you initialize the Smart Protection Server 3.2 computer. After initializing the Smart Protection Server 3.2 computer, you can no longer migrate settings unless you uninstall and reinstall the server.

For a complete list of prerequisites required to begin migrating, see [Migrating Settings Prerequisites on page A-2](#).

Procedure

1. Open a command line on the Smart Protection Server 3.2 virtual machine using root account credentials.
2. Change the working directory to `/usr/tmcss/bin/MigrationTool`.
3. Execute the Migration Tool using the following command:

```
#> ./Migration.py
```

The Migration Tool requests server information.

```
root@localhost:/usr/tmcss/bin/MigrationTool
[root@localhost MigrationTool]# pwd
/usr/tmcss/bin/MigrationTool
[root@localhost MigrationTool]# ./Migration.py
Welcome to use SPS Migration Tool
Server location: █
```

4. Provide the **Server location** of the Smart Protection Server computer that you want to migrate settings from.

**Note**

The **Server location** supports IP address or FQDN format and attempts to verify the location using an SSH connection.

```
root@localhost:/usr/tmcss/bin/MigrationTool
[root@localhost MigrationTool]# pwd
/usr/tmcss/bin/MigrationTool
[root@localhost MigrationTool]# ./Migration.py
Welcome to use SPS Migration Tool
Server location: 10.201.131.208
./Migration.py:33 - Server 10.201.131.208 connect successfully
SSH user(default: root):
```

5. To obtain the settings from the previous server, provide the root account and password.

The migration process begins. Depending on the size of the database, the migration process may take some time to complete. After the migration process

completes successfully, the Smart Protection Server 3.2 computer automatically reboots and applies the migrated settings.

```

root@localhost:/usr/tmcss/bin/MigrationTool
GRANT
GRANT
REVOKE
REVOKE
GRANT
GRANT
./Migration.py:301 - Import postgres data might failed
./Migration.py:105 - End to migrate_postgres
./Migration.py:100 - Start to migrate chkconfig

Note: This output shows SysV services only and does not include native
systemd services. SysV configuration data might be overridden by native
systemd configuration.

If you want to list systemd services use 'systemctl list-unit-files'.
To see services enabled on particular target use
'systemctl list-dependencies [target]'.

./Migration.py:271 - chkconfig svaipables on
./Migration.py:271 - chkconfig lighttpd on
./Migration.py:271 - chkconfig jetty.sh on
./Migration.py:271 - chkconfig svanetwork on
./Migration.py:271 - chkconfig lwcscd on
./Migration.py:271 - chkconfig jexec on
./Migration.py:271 - chkconfig ssfbd on
./Migration.py:105 - End to migrate chkconfig
./Migration.py:100 - Start to migrate solr
Starting Jetty: STARTED Jetty Tue Feb 14 17:44:04 CST 2017
./Migration.py:223 - waiting solr init finished...
2017-02-14 17:44:05.078::INFO: Logging to STDERR via org.mortbay.log.StdErrLog
2017-02-14 17:44:05.223::INFO: Redirecting stderr/stdout to /var/tmcss/debuglogs/jetty.log
Stopping Jetty: OK
./Migration.py:105 - End to migrate_solr
./Migration.py:339 - Migrate successfully!!
./Migration.py:340 - System Reboot!!
Shutdown scheduled for Tue 2017-02-14 17:45:20 CST, use 'shutdown -c' to cancel.
[root@localhost MigrationTool]#
Broadcast message from root@localhost.localdomain (Tue 2017-02-14 17:44:20 CST):

The system is going down for reboot at Tue 2017-02-14 17:45:20 CST!

[root@localhost MigrationTool]#

```



Important

If an issue occurs during the migration process, Smart Protection Server does not reboot and a list of error messages appears. You can obtain the migration error log file in the following location:

```
/var/tmcss/debuglogs/SPSMigration.log
```

6. Open the Smart Protection Server 3.2 console using the admin account and verify the migrated settings.

- Check the pattern status for File Reputation and Web Reputation Services:
 - a. Go to **Updates > Pattern**.
 - b. Ensure that **File Reputation** and **Web Reputation** are correctly configured.
 - c. If a pattern was incorrectly disabled, click **Update Now** to obtain the latest pattern.

**Note**

If the update is unsuccessful, check that you can access the Internet and that your proxy settings are correct (**Administration > Proxy Settings**).

- Check that **Synchronize and enable suspicious objects** are correctly configured by going to **Smart Protection > Suspicious Objects**.

**Note**

If **Synchronize and enable suspicious objects** is incorrectly disabled, confirm the **Source** and **API key** information of the virtual analyzer source and click **Subscribe**.

- Check all other settings in the Smart Protection Server web console.
7. If the previous Smart Protection Server 3.x computer required certificates, you must re-import the certificates.

**Note**

For more information, see the Smart Protection Server Administrator's Guide.

8. To continue using the same IP address of your previous version of Smart Protection Server on the Smart Protection Server 3.2 console, shut down the previous version of Smart Protection Server.
-

Index

D

documentation feedback, 4-6

document conventions, v

S

support

 resolve issues faster, 4-4

T

Trend Micro

 about, iv



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: APEM37757/170322