TREND MICRO™

3.3 TREND MICRO™ Smart Protection Server

Installation and Upgrade Guide

Security Made Smarter

Endpoint Security

Messaging Security

Protected Cloud

Web Security

Document Part No.: APEM37915/170817

Release Date: October 2017

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

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

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

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:

https://www.trendmicro.com/download/documentation/rating.asp

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Smart Protection Server collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Preface

Preface

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

Topics include:

About Trend Micro

Trend Micro provides virus protection, antispam, 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:

https://docs.trendmicro.com/en-us/enterprise/smart-protection-server.aspx

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

The following table lists the system requirements:

HARDWARE/ SOFTWARE	REQUIREMENTS
Hardware	• 2.0 GHz Intel™ Core2 Duo™ 64-bit processor supporting Intel™ Virtualization Technology™ or equivalent • 2 GB of RAM (Trend Micro recommends 4 GB) • 50 GB disk space when installed on a virtual machine **Note** Smart Protection Server automatically partitions the detected disk space as required. **Note** The Blocked URLs stop collecting data if Smart Protection Server detects that the available disk space is less than 1 GB. Smart Protection Server starts collecting data again once the administrator has made at least 1.5 GB of disk space available. • Monitor with 1024 x 768 or greater resolution with 256 colors or higher

Hardware/ Software	Requirements
Virtualization	• 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™ 7.2, 7.1, 6.5 **Note** If you use a Citrix™ XenServer, create a new Virtual Machine using the Other install media template. **Note** Smart Protection Server already has a purpose-built, hardened, performance-tuned 64-bit Linux operating system.

HARDWARE/ SOFTWARE	REQUIREMENTS
Virtual Machine	• CentOS 7 64-bit or CentOS 64-bit • Allocate at least 2 GB of RAM to the Virtual Machine. Trend Micro recommends you allocate 4 GB. • 2.0 GHz processor • 2 virtual processors minimum (4 virtual processors recommended) • 50 GB disk space • 1 network device • Network Device **Note** 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. 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.
Web Console	• 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 • Google Chrome™

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

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 3.1, a command line Migration Tool allows you to transfer preconfigured settings to Smart Protection Server 3.3.

For a complete list of prerequisites required to begin migrating, see *Migrating Settings Prerequisites on page A-2*. For more information, see *Migrating Settings from Smart Protection Server 3.1 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

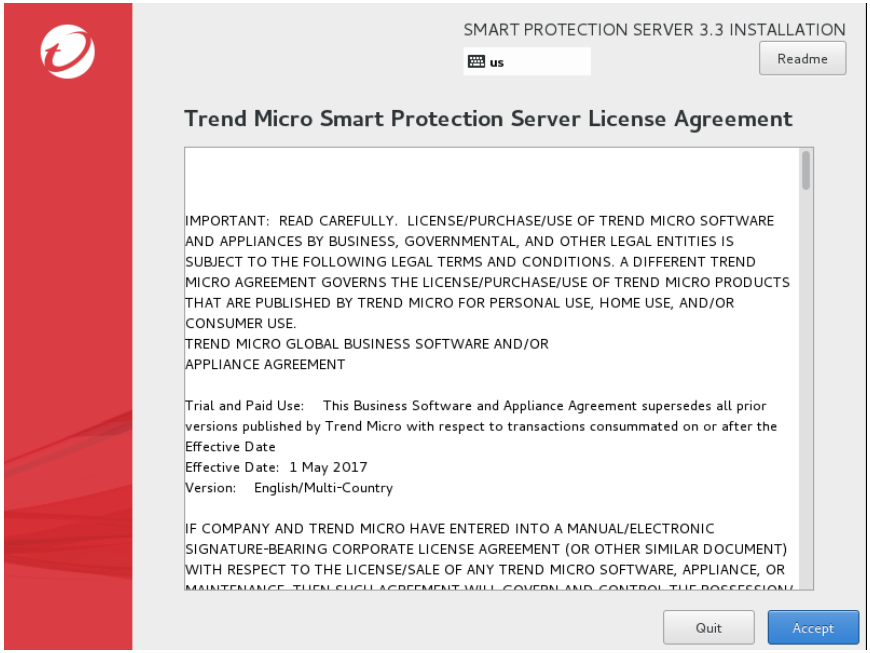
   For more information, refer to the Virtual Machine section in *System Requirements on page 1-2*.

2. Power on the virtual machine.

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

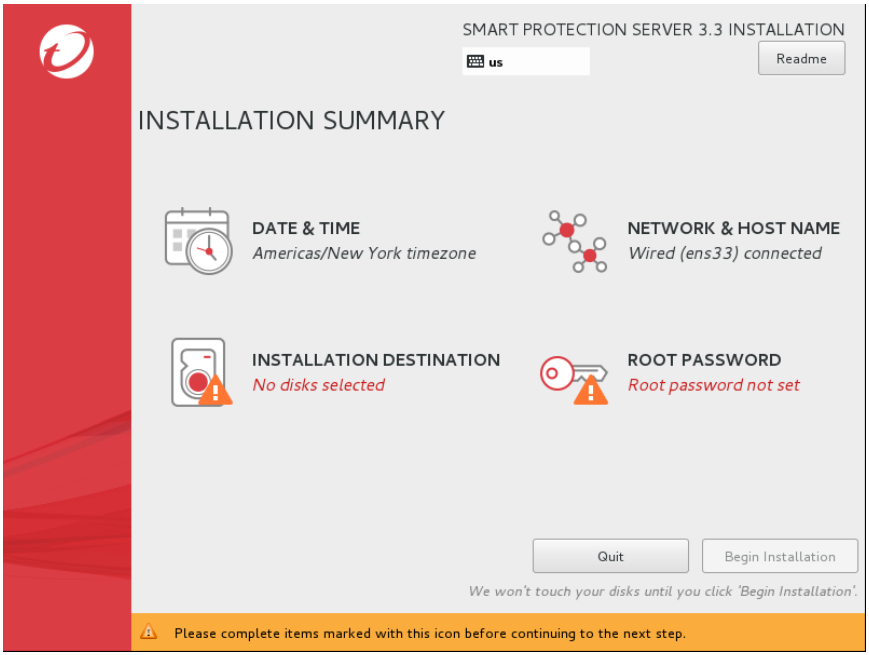
3. Select the language for this installation of Smart Protection Server.
4. Click **Continue**.

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 customize the date and time, select your **Region** and **City** from the dropdown lists, or click your region on the map.

   b. 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

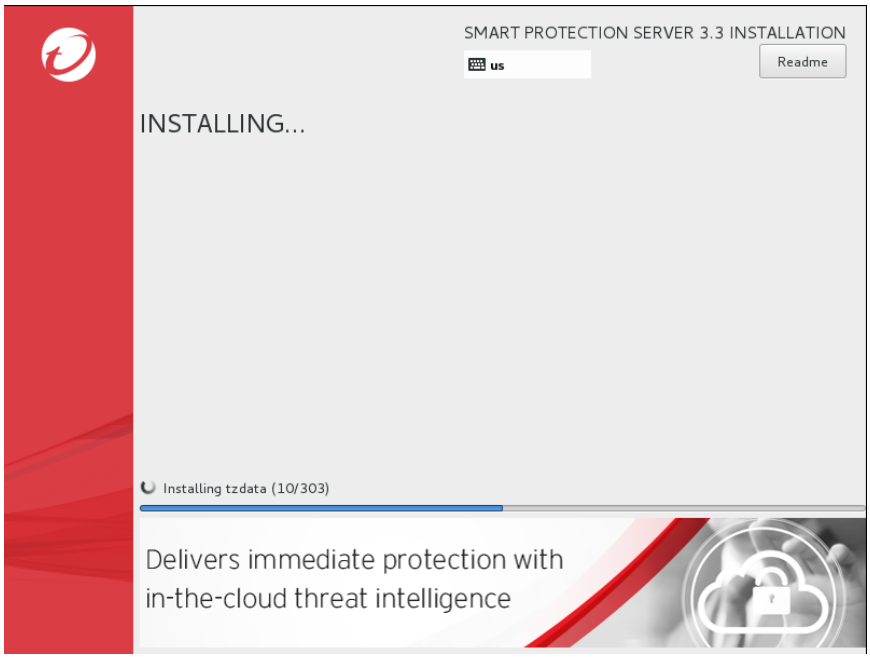
a. Click **Done**.

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 3.1, use the command line Migration Tool to transfer preconfigured settings to Smart Protection Server 3.3.

Note

For more information, see *Migrating Settings from Smart Protection Server 3.1 on page A-2*.

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*.

Upgrading

Upgrade to this version of Smart Protection Server from Smart Protection Server 3.2.

TABLE 2-1. Version Upgrade Details

VERSION	REQUIREMENTS
Upgrading to Smart Protection Server 3.3	• Ensure that System Requirements are met before installation. See *System Requirements on page 1-2*. • Smart Protection Server 3.2 • Clear the browser's temporary Internet files before logging on to the web console.

The web service is disabled for about 5 minutes during the upgrade process. During this time, endpoints will not be able to send queries to Smart Protection Server. Trend Micro recommends redirecting endpoints to another Smart Protection Server for the duration of the upgrade. If there is only one Smart Protection Server installed on your network, Trend Micro recommends planning the upgrade for off-peak times. Suspicious files will

be logged and scanned immediately once connection to Smart Protection Server is restored.

Note

SOCKS4 proxy configuration has been removed from Smart Protection Server. After upgrading to this version, if in the previous version SOCKS4 was configured for the proxy settings, the proxy settings need to be re-configured.

Upgrading Smart Protection Server

Procedure

1. Log on to the web console.
2. Click **Updates** from the main menu.

   A drop down menu appears.
3. Click **Program**.

   The Program screen appears.
4. Under Upload Component, click **Browse**.

   The **Choose File to Upload** screen appears.
5. Select the upgrade file from the Choose File to Upload screen.
6. Click **Open**.

   The Choose File to Upload screen closes and the file name appears in the Upload program package text box.
7. Click **Update**.
8. Perform post installation tasks.

   Refer to *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

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 3.1, execute the Smart Protection Server Migration Tool (Migration.py) to transfer all of your settings to Smart Protection Server 3.3 before continuing.

For more information, refer to *Migrating Settings from Smart Protection Server 3.1 on page A-2*.

Procedure

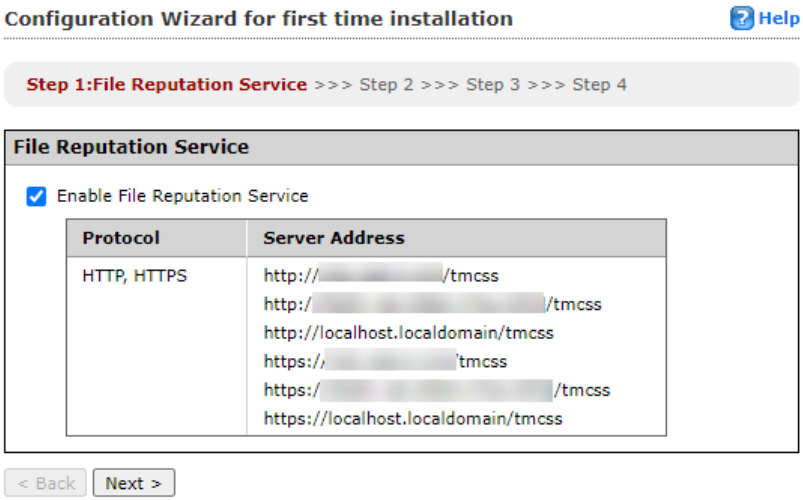
1. Log on to the web console.

   The **Welcome** screen appears.

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

   The first time installation wizard appears.

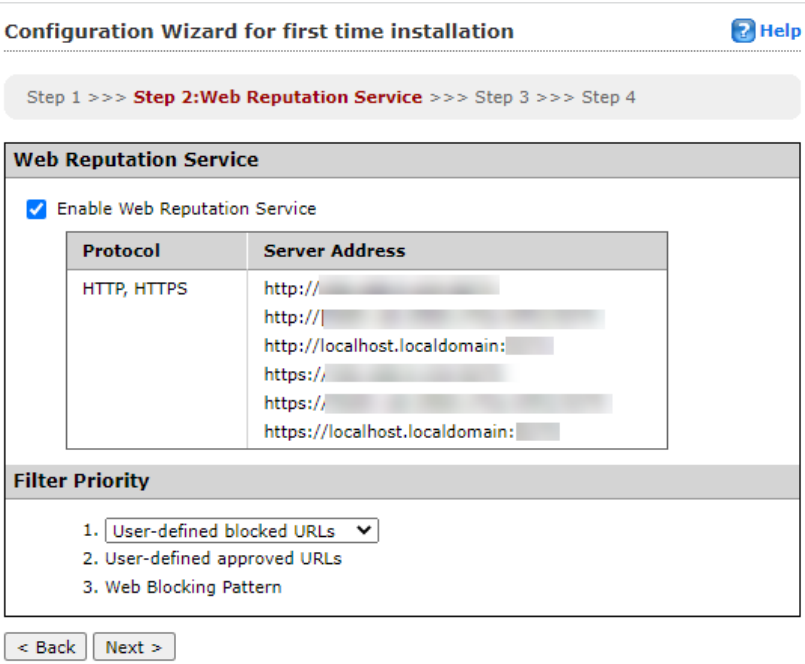
3. Select the **Enable File Reputation Service** check box.



4. Click **Next**.

   The Web Reputation Service screen appears.

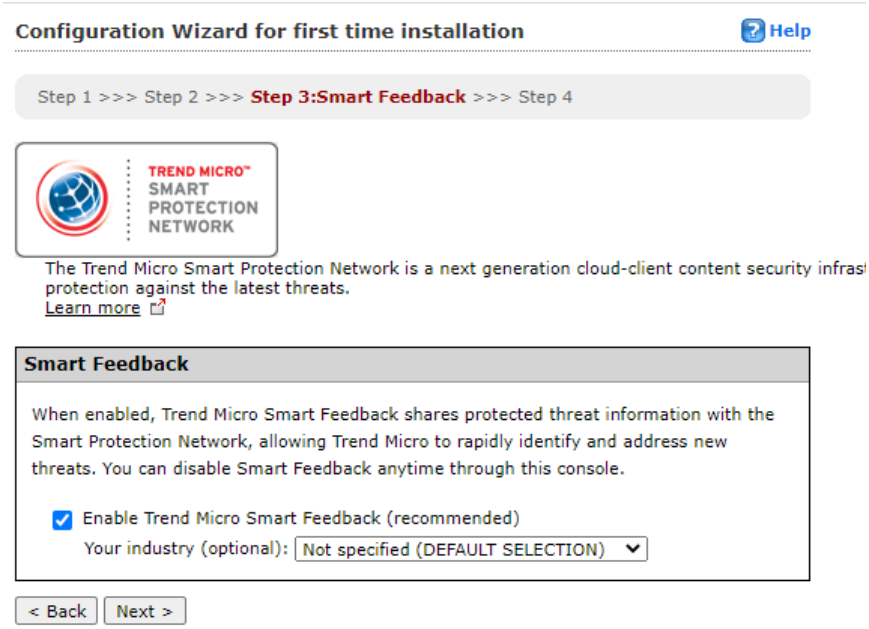
5. Select the **Enable Web Reputation Service** check box.



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

7. Click **Next**.

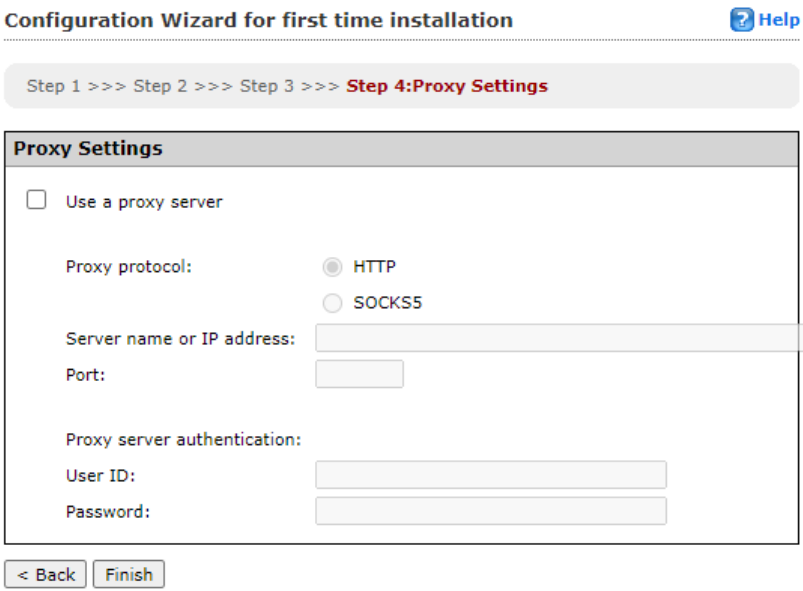
The Smart Feedback screen appears.



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

9. Click **Next**.

The Proxy Settings screen appears.



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

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

Using the Support Portal

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

Procedure

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

   Tip

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

   https://success.trendmicro.com/smb-new-request

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

Threat Encyclopedia

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

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

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

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

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone 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	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

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

- Trend Micro product documentation:

https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://www.ers.trendmicro.com/

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

https://success.trendmicro.com/solution/1112106

File Reputation Services

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

https://success.trendmicro.com/solution/1059565

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Other Resources

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

Download Center

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

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

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

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:

https://docs.trendmicro.com/en-us/survey.aspx

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

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

Important

You can only migrate settings from previous Smart Protection Server versions before you initialize Smart Protection Server 3.3. After initializing Smart Protection Server 3.3, 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	• Smart Protection Server 3.3 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 3.3 ISO must be installed on the virtual machine instance before running the tool.
SSH	SSH must be enabled on the Smart Protection Server computer that you want to migrate settings from. For more information, see the Online Help or Administrator's Guide.
Suspicious Object synchronization	If Suspicious Objects synchronization is enabled, ensure that there is a working connection between the new virtual machine and the Suspicious Objects source.

Migrating Settings from Smart Protection Server 3.1

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

Important

You can only migrate settings from previous Smart Protection Server versions before you initialize Smart Protection Server 3.3. After initializing Smart Protection Server 3.3, 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 3.3 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.
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.
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, Smart Protection Server 3.3 automatically reboots and applies the migrated settings.

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 3.3 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 3.1 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 3.3 console, shut down the previous version of Smart Protection Server.

Index

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: APEM37915/170817