



3.0 TREND MICRO™ Smart Protection Server

Installation and Upgrade 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://downloadcenter.trendmicro.com/>

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 © 2014. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM36293/140116

Release Date: July 2014

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 and Upgrading Smart Protection Server

Performing a Fresh Installation	2-2
Installing Smart Protection Server	2-2
Upgrading	2-14
Upgrading to Smart Protection Server	2-15

Chapter 3: Post-Installation Tasks

Post-Installation	3-2
Initial Configuration	3-2

Chapter 4: Getting Help

Frequently Asked Questions	4-2
How do I log on to the Command Line Interface (CLI)?	4-2
Why Does the Smart Protection Server IP Address Disappear When I Use the CLI to Enable Hyper-V Integration Components on a Non-Hyper-V Machine?	4-2
Can Other Linux Software Be Installed on the Smart Protection Server?	4-4
How Do I Change the Smart Protection Server IP Address?	4-4
How Do I Change the Smart Protection Server Hostname?	4-5
How Do I Perform an Upgrade If a Pattern is Updating?	4-5
How Do I Configure the NTP Server?	4-6
Using the Support Portal	4-6
Known Issues	4-7
Hot Fixes, Patches, and Service Packs	4-7
Threat Encyclopedia	4-8
Contacting Trend Micro	4-8
Speeding Up the Support Call	4-9
TrendLabs	4-10

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 Incorporated 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:

<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 Trend Micro™ 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 RAM• 30GB or 35GB (recommended) disk space when installed on a virtual machine <hr/> <div data-bbox="420 672 467 711"></div> <div data-bbox="475 672 530 695">Note</div> <div data-bbox="475 711 1091 760">Smart Protection Server automatically partitions the detected disk space as required.</div> <hr/> <div data-bbox="420 821 467 860"></div> <div data-bbox="475 821 530 842">Note</div> <div data-bbox="475 859 1091 990">The Blocked Web Access log stops 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"> <li data-bbox="467 282 1022 310">• Microsoft™ Windows Server™ 2008 R2 Hyper-V™ <hr/> <div data-bbox="516 355 561 394"></div> <div data-bbox="575 355 626 376" style="color: red;">Note</div> <div data-bbox="575 394 1143 444">Install the Legacy Network Adapter to detect the network device for Hyper-V installations.</div> <div data-bbox="575 466 1163 544">After installing Smart Protection Server, use the Command Line Interface (CLI) to enable Hyper-V Integration Components to increase capacity.</div> <hr/> <li data-bbox="467 573 986 600">• Microsoft™ Windows Server™ 2012 Hyper-V™ <hr/> <div data-bbox="516 646 561 685"></div> <div data-bbox="575 646 626 667" style="color: red;">Note</div> <div data-bbox="575 685 1143 735">Install the Legacy Network Adapter to detect the network device for Hyper-V installations.</div> <hr/> <li data-bbox="467 764 1022 792">• Microsoft™ Windows Server™ 2012 R2 Hyper-V™ <hr/> <div data-bbox="516 837 561 876"></div> <div data-bbox="575 837 626 859" style="color: red;">Note</div> <div data-bbox="575 876 1143 927">Install the Legacy Network Adapter to detect the network device for Hyper-V installations.</div> <hr/> <ul style="list-style-type: none"> <li data-bbox="467 956 1180 1006">• VMware™ ESXi™ Server 5.5, 5.1, 5.0 Update 2, 4.1 Update 1, 4.0 Update 3, or 3.5 Update 4 <li data-bbox="467 1027 1112 1078">• VMware™ ESX™ Server 4.1 Update 1, 4.0 Update 3, or 3.5 Update 4 <li data-bbox="467 1099 888 1127">• Citrix™ XenServer™ 6.2, 6.0, and 5.6 <hr/> <div data-bbox="516 1172 561 1211"></div> <div data-bbox="575 1172 626 1193" style="color: red;">Note</div> <div data-bbox="575 1211 1099 1261">If you use a Citrix™ XenServer, create a new Virtual Machine using the Other install media template.</div> <hr/> <div data-bbox="516 1320 561 1359"></div> <div data-bbox="575 1320 626 1341" style="color: red;">Note</div> <div data-bbox="575 1359 1184 1409">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 5 64-bit (Guest Operating System) If your VMWare version (such as 3.5 and 4.0) does not support CentOS, use Red Hat™ Enterprise Linux™ 5 64-bit <hr/> <p> Note Only Virtual NIC E1000 and VMware VMXNET3 NICs are supported.</p> <hr/> <ul style="list-style-type: none"> 2GB RAM 2.0GHz processor 30GB or 35GB (recommended) disk space when installed on a virtual machine 1 network device 2 virtual processors minimum (4 virtual processors recommended) Network Device <hr/> <p> 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.</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>
Web Console	<ul style="list-style-type: none"> Microsoft™ Internet Explorer™ 7.0 or later with the latest updates 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 Servers.

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 Servers 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):

```
service lighttpd restart
```

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 Servers 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 Servers to use for your network, you can begin the installation process.



Tip

Install multiple Smart Protection Servers 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 and Upgrading Smart Protection Server

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

Topics include:

- *Performing a Fresh Installation on page 2-2*
- *Upgrading on page 2-14*

Performing a Fresh Installation

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

Installing Smart Protection Server

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.

Refer to the Virtual Machine section in [System Requirements on page 1-2](#) for more information about the type of virtual machine required for installation.



Note

A Legacy Network Adapter is required to detect the network device for Hyper-V installations.

2. Power on the virtual machine.

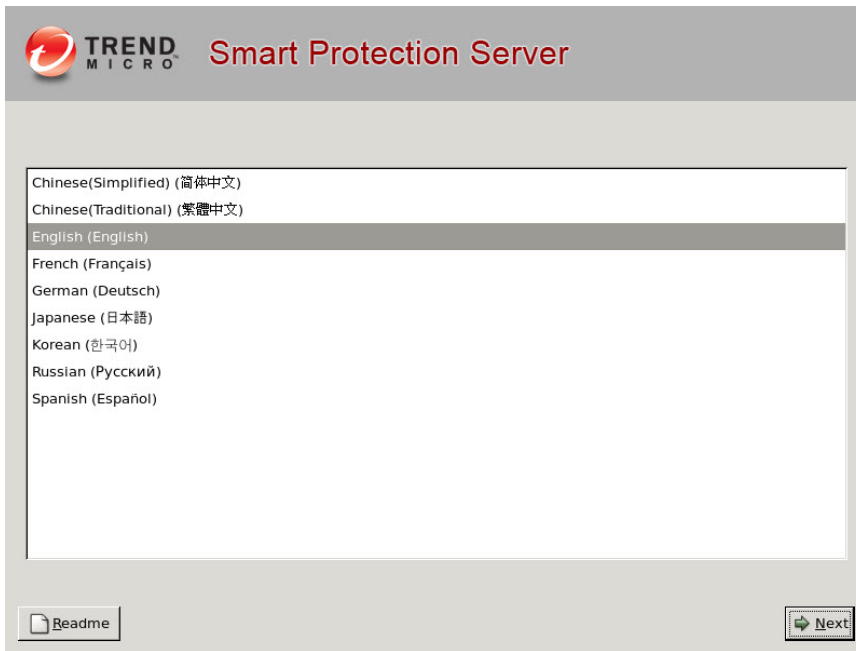
The Installation Menu displays with the following options:

- **Install Smart Protection Server:** Select this option to install Smart Protection Server to the new virtual machine.
- **System Memory Test:** Select this option to perform memory diagnostic tests to rule out any memory issues.
- **Exit Installation:** Select this option to exit the installation process and to boot from other media.



3. Select **Install Smart Protection Server**.

The Select language screen appears.



Note

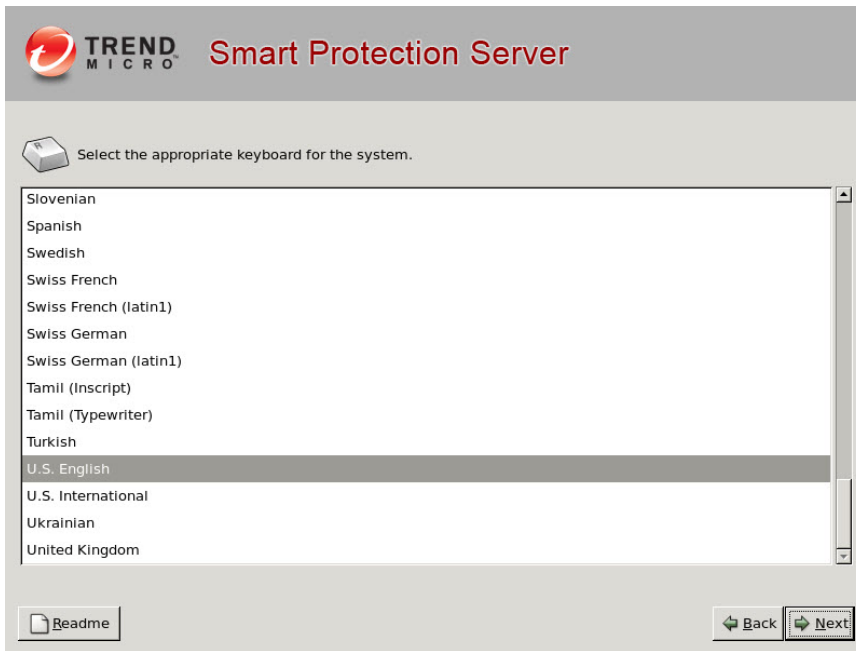
From this screen on, you can access the readme from a button in the lower left hand corner of the installation screen.

4. Select the language for this installation of Smart Protection Server and click **Next**.
The License Agreement screen appears.



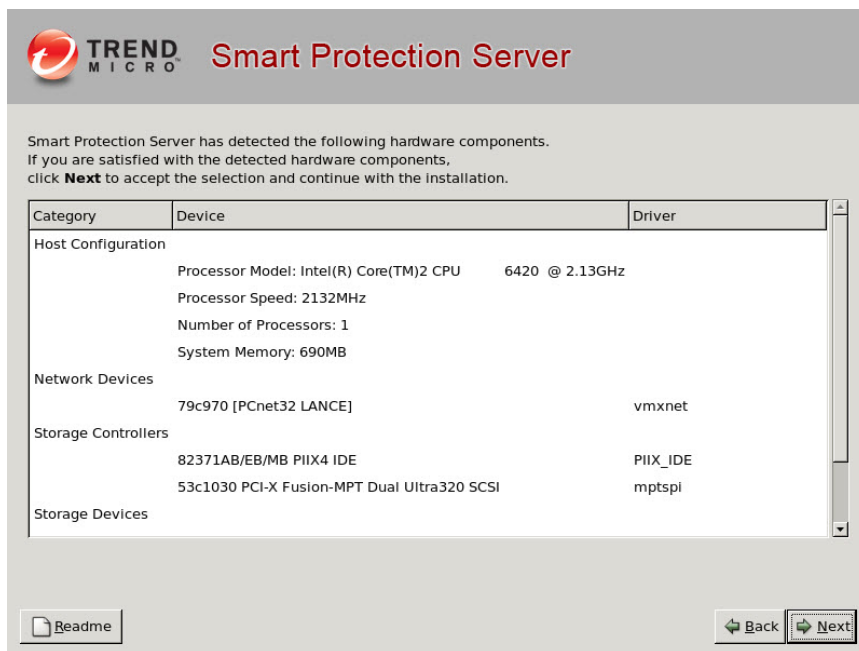
5. Click **Accept** to continue.

The Keyboard Selection screen appears.



6. Select the keyboard language and click **Next** to continue.

The Hardware Components Summary screen appears.



The installation program performs a scan to determine if the system specifications have been met and displays the results. If the hardware contains components that do not meet the system requirements, the installation program highlights those components. Installation can proceed as long as there is a hard drive and network device. If there is no hard drive or no network device, installation cannot continue.

7. Click **Next** to continue.

The Network Settings screen appears.

TREND MICRO Smart Protection Server

Network Devices

Active on Boot	Device	Description	IPv4/Ne	Edit
<input type="radio"/>	eth0	Digital Equipment Corporation DECchip 21140 [FasterNet]	10.201.	

Hostname

Set the host name:

☐ Automatically via DHCP

☒ Manually (e.g., host.domain.com)

Miscellaneous Settings

IPv4		IPv6	
Gateway	<input type="text"/>	Gateway	<input type="text"/>
Primary DNS	<input type="text"/>	Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>	Secondary DNS	<input type="text"/>



Note

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

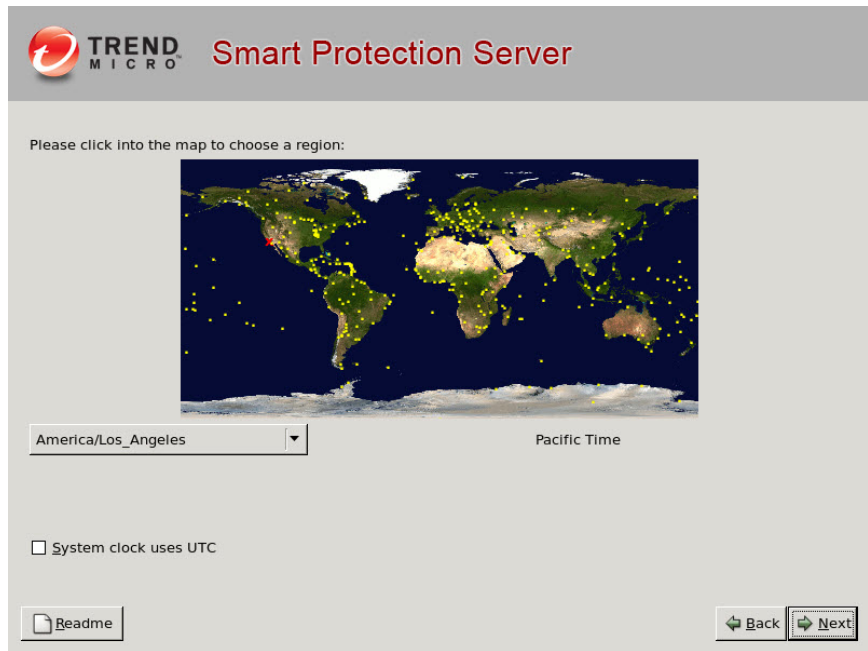
If there are multiple network devices, configure settings for all devices. (Only one device can be active on boot.)

8. Specify the Active on Boot network devices, host name, and miscellaneous settings.

The **Edit** 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 DHCPv6.

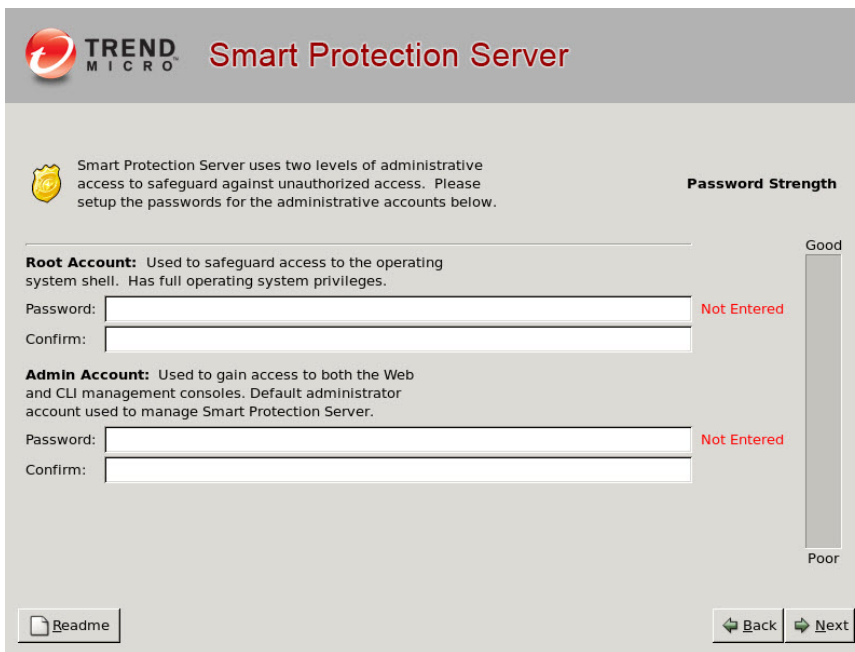
9. Click **Edit** to select manual configuration and configure miscellaneous settings.
10. Click **Next** to continue.

The Time Zone screen appears.



11. Specify the time zone.
12. Click **Next** to continue.

The Authentication screen appears.



The screenshot shows the 'Smart Protection Server' installation window. At the top is the Trend Micro logo and the title 'Smart Protection Server'. Below the logo, a shield icon with a keyhole is next to the text: 'Smart Protection Server uses two levels of administrative access to safeguard against unauthorized access. Please setup the passwords for the administrative accounts below.' To the right of this text is a 'Password Strength' indicator, which is a vertical bar with 'Good' at the top and 'Poor' at the bottom. The bar is currently empty, and the text 'Not Entered' is displayed in red next to the password fields for both accounts.

Root Account: Used to safeguard access to the operating system shell. Has full operating system privileges.

Password: Confirm:

Admin Account: Used to gain access to both the Web and CLI management consoles. Default administrator account used to manage Smart Protection Server.

Password: Confirm:

At the bottom left is a 'Readme' button with a document icon. At the bottom right are 'Back' and 'Next' buttons with left and right arrow icons respectively.

13. Specify passwords.

Smart Protection Server uses two different levels of administrator types to secure the server, the **root** and **admin** passwords.

- **Root account:** This 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 account:** This 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**

The password must be a minimum of 6 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.

14. Click **Next** to continue.

The Installation Summary screen appears.

TREND MICRO Smart Protection Server

Summary:

Language:	English
Keyboard:	U.S. English
Mouse:	No - mouse
Hostname:	spsserver-0000000000000000
Network Devices:	
Card:	Digital Equipment Corporation DECchip 21140 [FasterNet]
Device:	eth0
IPv4 Address:	192.168.1.100
Subnet mask:	255.255.255.0
Gateway:	192.168.1.1
Primary DNS:	192.168.1.1
IPv6 Address:	2001:db8:1:1::1

If you are satisfied with the configuration settings, click **Next** to continue with the installation. Smart Protection Server will format and partition the necessary hard disk space and install the operating system and application.

To change any configuration settings, click **Back**.

To cancel the installation, click **Cancel**.

Readme

Back **Cancel** **Next**

15. Confirm the summary information.

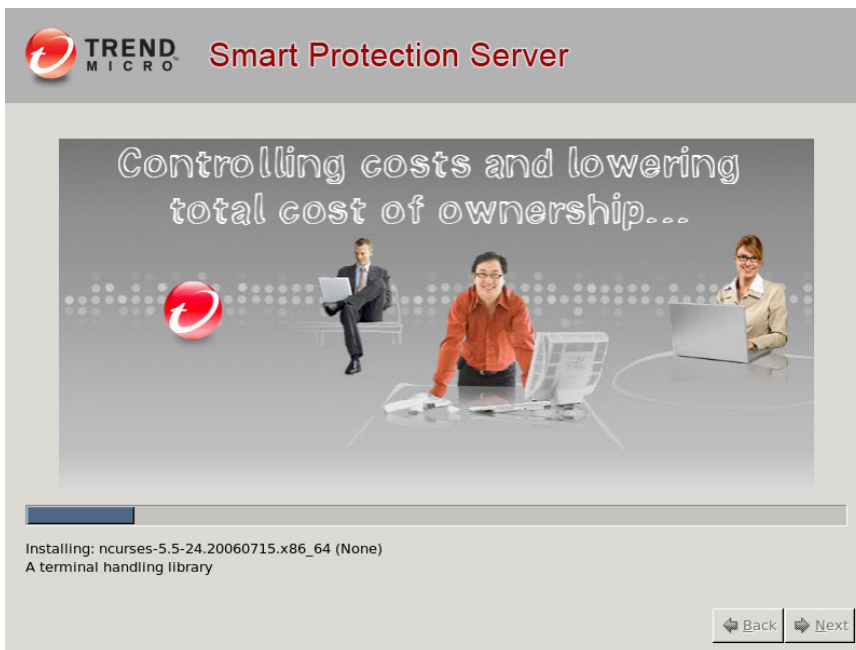
**Note**

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.

If any of the information on this screen requires a different configuration, click **Back**.

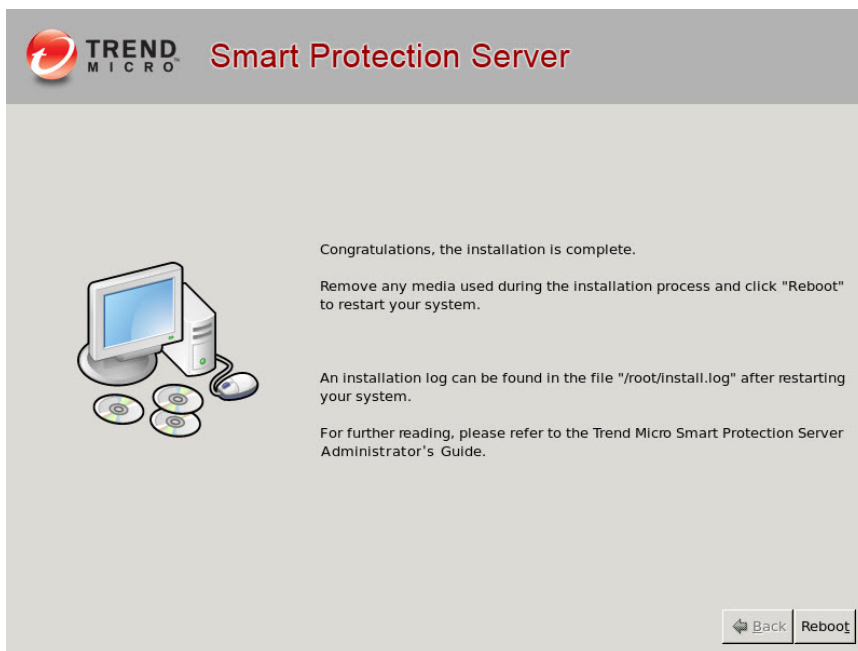
16. Click **Next** to continue and click **Continue** at the confirmation message.

The Installation Progress screen appears.



17. A message appears when the installation completes.

The installation log is saved in the `/root/install.log` file for reference.



18. Click **Reboot** to restart the virtual machine.

The initial product Command Line Interface (CLI) logon screen appears and displays the client connection addresses and the web console URL.



Note

Trend Micro recommends disconnecting the CD ROM device from the virtual machine after Smart Protection Server is installed.

19. Use **admin** to log on to the product CLI or the web console to manage Smart Protection Server. Log on to the web console to perform post installation tasks such as configuring proxy settings. Log on to the CLI shell if you need to perform additional configuration, troubleshooting, or maintenance tasks.



Note

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

20. Perform post installation tasks.

Refer to *Post-Installation Tasks on page 3-1*

Upgrading

Upgrade to this version of Smart Protection Server from Smart Protection Server 2.6, 2.5, 2.1 or 2.0.

TABLE 2-1. Version Upgrade Details

VERSION	REQUIREMENTS
Upgrading to Smart Protection Server 3.0	<ul style="list-style-type: none">• Ensure that System Requirements are met before installation. See <i>System Requirements on page 1-2</i>.• Smart Protection Server 2.0, 2.1, 2.5, or 2.6• Clear the browsers 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 to 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 Trend Micro™ 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:

- After installing Smart Protection Server with Hyper-V, enable Hyper-V Integration Components to increase capacity. Ensure that a Network Adapter is available before enabling Hyper-V Integration Components. Enable Hyper-V Integration Components from the Command Line Interface (CLI) with your admin account by typing:

```
enable
enable hyperv-ic
```

- 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.

Procedure

1. Log on to the web console.
The first time installation wizard appears.
2. 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

< Back

Next >

3. Click **Next**.
The Web Reputation Service screen appears.
4. Select the **Enable Web Reputation Service** check box to enable Web Reputation.

The screenshot shows the 'Configuration Wizard for first time installation' window. At the top, there's a progress bar with four steps: Step 1, Step 2: Web Reputation Service (highlighted in red), Step 3, and Step 4. Below the progress bar is the 'Web Reputation Service' section. It contains a checkbox labeled 'Enable Web Reputation Service' which is checked. Below this is a table with two columns: 'Protocol' and 'Server Address'. The table has three rows, all with 'HTTP' in the Protocol column. The Server Address column contains three entries: 'http://10.1.123.456:8080 (IPv4 address)', 'http://[fd10:1234:5678:1:2e1e:fd10:a456:c7d1]:8080 (IPv6 address)', and 'http://localhost.localdomain:8080'. Below the table is the 'Filter Priority' section, which lists three items: '1. Blocked URLs' (with a dropdown arrow), '2. Approved URLs', and '3. Web Blocking List'. At the bottom of the window are two buttons: '< Back' and 'Next >'. A 'Help' icon is visible in the top right corner.

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://10.1.123.456:8080 (IPv4 address)
HTTP	http://[fd10:1234:5678:1:2e1e:fd10:a456:c7d1]:8080 (IPv6 address)
HTTP	http://localhost.localdomain:8080

Filter Priority

1. Blocked URLs ▼
2. Approved URLs
3. Web Blocking List


< Back Next >

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

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

9. Specify proxy settings if your network uses a proxy server.
10. 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

Getting Help

This chapter includes details on how to get additional help while working with Trend Micro™ Smart Protection Server™.

Topics include:

- *Using the Support Portal on page 4-6*
- *Threat Encyclopedia on page 4-8*
- *Contacting Trend Micro on page 4-8*
- *TrendLabs on page 4-10*

Frequently Asked Questions

How do I log on to the Command Line Interface (CLI)?

CLI commands allow administrators to perform configuration tasks and to perform debugging and troubleshooting functions.

Administrators can log on to CLI through CLI or the SSH console using the **admin** account through the SSH connection.

Why Does the Smart Protection Server IP Address Disappear When I Use the CLI to Enable Hyper-V Integration Components on a Non-Hyper-V Machine?

Microsoft™ Hyper-V Integration Components should only be enabled on Microsoft™ Hyper-V machines. The Smart Protection Server IP address no longer appears if Hyper-V Integration Components are enabled on a non-Hyper-V machine as illustrated here. If

Hyper-V Integration Components are enabled on a non Hyper-V machine, you will not be able to connect to Smart Protection Server through the network.

```
Trend Micro Smart Protection Server

Use one of the following addresses with your Trend Micro client management
products for File Reputation connections:

https:///tmcss
http:///tmcss

Use the following address with your Trend Micro client management products
for Web Reputation connections:

http://:5274

Use the following URL to access the Web product console:

https://:4343

You will be prompted for your administrator account and password.
Please have your administrator account and password ready for authentication.

Use the following log on prompt to access the Command Line Interface (CLI):

test login:
```

FIGURE 4-1. IP address no longer appears



Note

On Microsoft™ Hyper-V machines, the IP address may disappear if a network adapter is not connected.

Rolling Back the Network Setting

Procedure

1. Log on to the Command Line Interface (CLI) using **admin**.
2. Type the following commands:

```
enable  
configure service interface eth0
```

Can Other Linux Software Be Installed on the Smart Protection Server?

Trend Micro does not recommend installing other Linux software on the Smart Protection Server virtual environment. Installing other Linux software may adversely affect the performance of the server and other applications might not work properly due to security settings on the Smart Protection Server.

How Do I Change the Smart Protection Server IP Address?

Changing an IPv4 Address

Procedure

1. Log on to the Command Line Interface (CLI) using **admin**.
2. Type the following commands:

```
enable  
configure ipv4 static <new ipv4 add> <subnet> <v4gateway>
```

3. Verify the changes by typing the following command:

```
show ipv4 address
```

4. Restart the machine.
-

Changing an IPv6 Address

Procedure

1. Log on to the Command Line Interface (CLI) using **admin**.
2. Type the following commands:

```
enable  
configure ipv6 static <new ipv6 add> <prefix> <v6gateway>
```

3. Verify the changes by typing the following command:

```
show ipv6 address
```

4. Restart the machine.
-

How Do I Change the Smart Protection Server Hostname?

Procedure

1. Log on to the Command Line Interface (CLI) using **admin**.
2. Type the following commands:

```
enable  
configure hostname <hostname>
```

3. Verify the changes by typing the following command:

```
show hostname
```

How Do I Perform an Upgrade If a Pattern is Updating?

Trend Micro recommends waiting until a pattern finishes updating before performing an upgrade. To prevent an update from occurring while upgrading disable scheduled updates.

Procedure

1. Log on to the Smart Protection Server web management console using **admin**.
 2. Click **Updates > Pattern**.
 3. Disable scheduled updates.
 4. Click **Save**.
-

**Note**

After performing an upgrade, remember to enable the scheduled updates.

How Do I Configure the NTP Server?

Procedure

1. Log on to the Command Line Interface (CLI) using **admin**.
2. Type the following commands:

```
enable  
configure ntp <ip or FQDN>
```

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 a product or service from the appropriate drop-down list and specify any other related information.

The **Technical Support** product page appears.

3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

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

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

Known Issues

Known issues document unexpected product behavior that might require a temporary work around. Trend Micro recommends always checking the readme file for information about system requirements and known issues that could affect installation or performance. Readme files also contain a description of what's new in a particular release, and other helpful information.

The latest known issues and possible workarounds can also be found in the Trend Micro Knowledge Base:

<http://esupport.trendmicro.com>

Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches and service packs to address outstanding issues, enhance product performance, and add new features.

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

- **Hot Fix:** a work-around or solution to customer-reported issues. Trend Micro develops and releases hot fixes to specific customers only.
- **Security Patch:** a single hot fix or group of hot fixes suitable for deployment to all customers
- **Patch:** a group of security patches suitable for deployment to all customers

- **Service Pack:** significant feature enhancements that upgrade the product

Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix, patch, and service pack releases:

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

All releases include a readme file that contains installation, deployment, and configuration information. Read the readme file carefully before performing installation.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined 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://www.trendmicro.com/vinfo> 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, fax, or email:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
---------	--

Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
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 hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.
- Virtualization platform (VMware™ or Hyper-V™) and version

TrendLabs

TrendLabsSM is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, 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.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

<http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs>



TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel: +1(408)257-1500 / 1-800 228-5651 Fax: +1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM36293/140116