



# 9.0 Worry-Free™ Business Security Standard and Advanced Editions Service Pack 1 Installation and Upgrade Guide

Securing Your Journey to the Cloud



Protected Cloud



Web Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, 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/smb/worry-free-business-security.aspx>

Trend Micro, the Trend Micro t-ball logo, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan, and ScanMail 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.: WFEM96625/140825

Release Date: September 2014

Protected by U.S. Patent No.: 5,951,698 and 7,188,369

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](mailto:docs@trendmicro.com).

Evaluate this documentation on the following site:

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



# Table of Contents

## Preface

Preface .....	v
Worry-Free Business Security Documentation .....	vi
Audience .....	vi
Document Conventions .....	vii

## Chapter 1: Preparing for Installation and Upgrade

Product Editions .....	1-2
Licenses, Registration, and Activation .....	1-3
The Worry-Free Business Security Network .....	1-5
Security Server .....	1-5
Agents .....	1-7
Web Console .....	1-7

## Chapter 2: Installing the Security Server

Installation and Upgrade Requirements .....	2-2
Security Server Installation Considerations .....	2-2
Security Server IPv6 Requirements .....	2-2
Location of the Security Server .....	2-3
Number of Clients .....	2-4
Network Traffic .....	2-4
Dedicated Server .....	2-5
Compatibility Issues .....	2-6
WFBS Ports .....	2-7
Installation Checklist .....	2-8
Installing the Security Server .....	2-12
Phase 1: Starting the Security Server Installation .....	2-14
Phase 2: Configuring Settings According to Setup Type .....	2-23
Configuring Settings for a Typical or Minimal Installation .....	2-23

Configuring Settings for a Custom Installation .....	2-28
Phase 3: Installation Process .....	2-50
Installing Several Security Servers Using Silent Installation .....	2-54
Recording an Installation Session .....	2-54
Starting the Silent Installation .....	2-56
Verifying the Installation .....	2-56

## **Chapter 3: Upgrading the Security Server and Agents**

Installation and Upgrade Requirements .....	3-2
Upgrade Considerations .....	3-2
IPv6 Requirements for Upgrades .....	3-2
Upgrade Best Practices .....	3-3
Previous Version Upgrades .....	3-3
Upgrade Method 1: Using the Installation Package to Upgrade .....	3-4
Upgrade Method 2: Move Agents to Security Server 9.0 SP1 .....	3-9
Upgrades to the Full Version or the Advanced Edition .....	3-11
Upgrading to the Full Version or the Advanced Edition .....	3-12

## **Appendix A: Getting Help**

The Trend Micro Knowledge Base .....	A-2
Contacting Technical Support .....	A-2
Case Diagnostic Tool .....	A-3
Speeding Up Your Support Call .....	A-3
Contact Information .....	A-3
Sending Suspicious Files to Trend Micro .....	A-4
Security Information Center .....	A-4
TrendLabs .....	A-5
Documentation Feedback .....	A-5

## **Index**

Index .....	IN-1
-------------	------





# Preface

## Preface

Welcome to the Trend Micro™ Worry-Free™ Business Security *Installation and Upgrade Guide*. This document discusses requirements and procedures for:

- Installing the Security Server
- Upgrading the Security Server and agents

For information on installing agents, see the *Administrator's Guide*.

# Worry-Free Business Security Documentation

Worry-Free Business Security documentation includes the following:

**TABLE 1. Worry-Free Business Security Documentation**

DOCUMENTATION	DESCRIPTION
Installation and Upgrade Guide	A PDF document that discusses requirements and procedures for installing the Security Server, and upgrading the server and agents
Administrator's Guide	A PDF document that discusses getting started information, client installation procedures, and Security Server and agent management
Help	HTML files compiled in WebHelp or CHM format that provide "how to's", usage advice, and field-specific information
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: <a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a>

Download the latest version of the PDF documents and readme at:

<http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx>

## Audience

Worry-Free Business Security documentation is intended for the following users:

- **Security Administrators:** Responsible for Worry-Free Business Security management, including Security Server and agent installation and management. These users are expected to have advanced networking and server management knowledge.

- **End users:** Users who have the Security Agent installed on their computers. The computer skill level of these individuals ranges from beginner to power user.

## Document Conventions

To help you locate and interpret information easily, the Worry-Free Business Security documentation uses the following conventions:

**TABLE 2. Document Conventions**

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
<b>Bold</b>	Menus and menu commands, command buttons, tabs, options, and tasks
<i>Italics</i>	References to other documentation or new technology components
<Text>	Indicates that the text inside the angle brackets should be replaced by actual data. For example, C:\Program Files \<file_name> can be C:\Program Files\sample.jpg.
 <b>Note</b>	Provides configuration notes or recommendations
 <b>Tip</b>	Provides best practice information and Trend Micro recommendations
 <b>WARNING!</b>	Provides warnings about activities that may harm computers on your network



# Chapter 1

## Preparing for Installation and Upgrade

This chapter discusses the preparations needed before installing or upgrading Worry-Free™ Business Security.

## Product Editions

Trend Micro offers the following editions:

- Worry-Free Business Security **Standard**: Designed to protect clients (desktops, portable computers, and servers) on your local network. This edition includes Outbreak Defense, Firewall, and Antivirus/Anti-spyware scanning. It also comes with technical support, malware/virus pattern file downloads, real-time scanning, and program updates for one year.
- Worry-Free Business Security **Advanced**: Designed to protect clients and Microsoft Exchange servers on your network. In addition to all the features in Worry-Free Business Security Standard, this edition includes Anti-spam, Content Filtering, Data Loss Prevention, and Attachment Blocking.

The following table lists the features supported for each edition.

**TABLE 1-1. Features Available by Product Editions**

FEATURES	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Component Updates	Yes	Yes
Device Control	Yes	Yes
Antivirus/Anti-spyware	Yes	Yes
Firewall	Yes	Yes
Web Reputation	Yes	Yes
URL Filtering	Yes	Yes
Behavior Monitoring	Yes	Yes
User Tools	Yes	Yes
Mail Scan (POP3)	Yes	Yes
Anti-Spam (POP3)	Yes	Yes
Mail Scan (IMAP)	No	Yes

FEATURES	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Anti-Spam (IMAP)	No	Yes
Email Message Content Filtering	No	Yes
Email Message Data Loss Prevention	No	Yes
Attachment Blocking	No	Yes

## Licenses, Registration, and Activation

When you purchase Worry-Free Business Security, you receive a license for the product(s) and a standard Maintenance Agreement. The standard Maintenance Agreement is a contract between your organization and Trend Micro regarding your right to receive technical support and product updates in consideration for the payment of applicable fees.

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase. After the first year, you must renew the Maintenance Agreement annually against then-current Trend Micro maintenance fees.



### Note

The Maintenance Agreement expires, but your License Agreement does not. If the Maintenance Agreement expires, scanning can still occur, but you will not be able to update the malware/virus pattern files, scan engine, or program files (even manually). Nor will you be entitled to receive technical support from Trend Micro.

Register and activate your Worry-Free Business Security license to enable the full functionality of the product.

### Registration Key

A Registration Key comes with your purchase of Worry-Free Business Security. It has 22 characters (including hyphens) and is in the following format:

xx-xxxx-xxxxx-xxxxx-xxxxx

Use a fully licensed Registration Key to register Worry-Free Business Security on the Trend Micro website at <https://clp.trendmicro.com>.

## Activation Code

After registering, you will receive a fully licensed Activation Code through email. An Activation Code has 37 characters (including the hyphens) and is in the following format:

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

During the Security Server installation, type the Activation Code when prompted. If you leave the field empty, Worry-Free Business Security installs the 30-day evaluation version. Upgrade to the fully licensed version before the evaluation version expires.

## License Status

The following table lists the features supported according to the license status.

**TABLE 1-2. License Status**

FEATURE	FULLY LICENSED	EVALUATION (30 DAYS)	EXPIRED
Expiration Notification	Yes	Yes	Yes
Component Updates	Yes	Yes	No
Program Updates	Yes	Yes	No
Technical Support	Yes	No	No
Real-time Scan	Yes	Yes	Yes but Real-time Scan will use outdated components

When a fully licensed Activation Code expires, you can no longer download scan engine or pattern file updates. However, unlike an evaluation version Activation Code, when a fully licensed version Activation Code expires, all existing configurations and other

settings remain in force. This provision maintains a level of protection in case you accidentally allow your license to expire.

You can renew a full version of Worry-Free Business Security by purchasing a maintenance renewal. You need an Activation Code to install the full versions.

If you have questions about the registration process, please consult the Trend Micro support website at:

<http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326>

## The Worry-Free Business Security Network

Worry-Free Business Security is comprised of the following:

- *Security Server on page 1-5*
- *Agents on page 1-7*
- *Web Console on page 1-7*

### Security Server

At the center of Worry-Free Business Security is the Security Server. The Security Server hosts the web console, the centralized web-based management console for Worry-Free Business Security. The Security Server installs agents to clients on the network and along with the agents, forms an agent-server relationship. The Security Server enables viewing security status information, viewing agents, configuring system security, and downloading components from a centralized location. The Security Server also contains the database where it stores logs of detected Internet threats being reported to it by the agents.

The Security Server performs these important functions:

- Installs, monitors, and manages agents.

- Downloads the components needed by agents. By default, the Security Server downloads components from the Trend Micro ActiveUpdate server and then distributes them to agents.

## Scan Server

The Security Server includes a service called Scan Server, which is automatically installed during Security Server installation. As such, there is no need to install it separately. The Scan Server runs under the process name `iCRCSERVICE.exe` and appears as **Trend Micro Smart Scan Service** from Microsoft Management Console.

When Security Agents use a scan method called **smart scan**, the Scan Server helps these agents run scans more efficiently. The smart scan process can be described as follows:

- The Security Agent scans the client for security threats using the **Smart Scan Agent Pattern**, a lightweight version of the traditional Virus Pattern. The Smart Scan Agent Pattern holds most of the threat signatures available on the Virus Pattern.
- A Security Agent that cannot determine the risk of the file during the scan verifies the risk by sending a scan query to the Scan Server. The Scan Server verifies the risk using the **Smart Scan Pattern**, which holds the threat signatures not available on the Smart Scan Agent Pattern.
- The Security Agent "caches" the scan query result provided by the Scan Server to improve the scan performance.

By hosting some of the threat definitions, the Scan Server helps reduce the Security Agents' bandwidth consumption when downloading components. Instead of downloading the Virus Pattern, Security Agents download the Smart Scan Agent Pattern, which is significantly smaller in size.

When Security Agents are unable to connect to the Scan Server, they send scan queries to the Trend Micro Smart Protection Network, which has the same function as the Scan Server.

It is not possible to uninstall the Scan Server separately from the Security Server. If you do not want to use the Scan Server:

1. On the Security Server computer, open Microsoft Management Console and disable the **Trend Micro Smart Scan Service**.

2. On the web console, switch Security Agents to conventional scan by navigating to **Preferences > Global Settings > Desktop/Server** tab and selecting the option **Disable Smart Scan Service**.

## Agents

Agents protect clients from security threats. Clients include desktops, servers, and Microsoft Exchange servers. The WFBS agents are:

**TABLE 1-3. WFBS Agents**

AGENT	DESCRIPTION
Security Agent	Protects desktops and servers from security threats and intrusions
Messaging Security Agent (Advanced only)	Protects Microsoft Exchange servers from email-borne security threats

An agent reports to the Security Server from which it was installed. To provide the Security Server with the very latest client information, the agent sends event status information in real time. Agents report events such as threat detection, startup, shutdown, start of a scan, and completion of an update.

## Web Console

The web console is the central point for monitoring clients throughout the corporate network. It comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console uses standard Internet technologies, such as Java, CGI, HTML, and HTTP.

Use the web console to:

- Deploy agents to clients.
- Organize agents into logical groups for simultaneous configuration and management.
- Configure product settings and start Manual Scan on a single group or on multiple groups.

- Receive notifications and view log reports for threat-related activities.
- Receive notifications and send outbreak alerts through email messages when threats are detected on clients.
- Control outbreaks by configuring and enabling Outbreak Defense.

## Chapter 2

# Installing the Security Server

This chapter provides information you will need to understand in order to install the Security Server.

## Installation and Upgrade Requirements

Visit the following website for a complete list of installation and upgrade requirements:

<http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx>

## Security Server Installation Considerations

Consider the following when installing the Security Server:

- *Security Server IPv6 Requirements on page 2-2*
- *Location of the Security Server on page 2-3*
- *Number of Clients on page 2-4*
- *Network Traffic on page 2-4*
- *Dedicated Server on page 2-5*
- *Compatibility Issues on page 2-6*

## Security Server IPv6 Requirements

The IPv6 requirements for the Security Server are as follows:

- The server must be installed on Windows Server 2008/2012, SBS 2008/2011, 7, 8, and Vista. It cannot be installed on Windows XP or Server/SBS 2003 because these operating systems only support IPv6 addressing partially.
- The server must use an IIS web server. Apache web server does not support IPv6 addressing.
- If the server will manage IPv4 and IPv6 agents, it must have both IPv4 and IPv6 addresses and must be identified by its host name. If a server is identified by its IPv4 address, pure IPv6 agents cannot connect to the server. The same issue occurs if pure IPv4 clients connect to a server identified by its IPv6 address.

- If the server will manage only IPv6 agents, the minimum requirement is an IPv6 address. The server can be identified by its host name or IPv6 address. When the server is identified by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.
- Verify that the host machine's IPv6 or IPv4 address can be retrieved using, for example, the “ping” or “nslookup” command.
- If you are installing the Security Server to a pure IPv6 computer, set up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the Security Server and the Internet to allow the server to successfully connect to Trend Micro hosted services, such as the ActiveUpdate server, the Online Registration website, and Smart Protection Network.

## Location of the Security Server

WFBS can accommodate a variety of network environments. For example, you can position a firewall between the Trend Micro Security Server and clients running the Security Agent, or position both the Trend Micro Security Server and all clients behind a single network firewall.

If more than one site is being managed, it is recommended that you install a Security Server at the main site, and at each managed site, to reduce bandwidth usage between the main site and managed sites, and to speed up pattern file deployment rates.

If clients have the Windows Firewall enabled, WFBS will automatically add it to the Exception list.



### Note

If a firewall is located between the Trend Micro Security Server and its clients, you must configure the firewall to allow traffic between the client listening port and Trend Micro Security Server's listening port.

---

## Number of Clients

A client is a computer where you plan to install a Security Agent or a Messaging Security Agent. This includes desktops, servers, and portable computers, including those that belong to users who telecommute.

A single Security Server installation can manage up to 2,500 clients. If you have more clients, Trend Micro suggests installing more than one Security Server.

## Network Traffic

WFBS generates network traffic when the Security Server and agents communicate with each other.

The Security Server/Scan Server generates traffic when:

- Notifying agents about configuration changes
- Notifying agents to download updated components
- Connecting to the Trend Micro ActiveUpdate server to check for and download updated components
- Responding to scan queries received from agents that use smart scan
- Sending feedback to the Trend Micro Smart Protection Network

Agents generate traffic when:

- Starting up
- Shutting down
- Generating logs
- Performing scheduled updates
- Performing manual updates (“Update Now”)
- Connecting to the Scan Server for scan queries

**Note**

Apart from updates, all the other actions generate a small amount of traffic.

---

## Network Traffic during Component Updates

The Security Server generates significant network traffic when it updates a component. To reduce network traffic generated during component updates, the Security Server performs component duplication. Instead of downloading an updated full pattern file, the Security Server only downloads the "incremental" patterns (smaller versions of the full pattern file) and merges them with the old pattern file after the download.

A Security Server that is updated regularly only downloads the incremental pattern. Otherwise, it downloads the full pattern file.

Trend Micro releases new pattern files regularly. Trend Micro also releases a new pattern file as soon as a damaging and actively circulating virus/malware is discovered.

## Using Update Agents to Reduce Network Bandwidth

If you identify sections of your network between Security Agents and the Security Server as "low-bandwidth" or "heavy traffic", you can specify Security Agents to act as update sources (Update Agents) for other agents. This helps distribute the burden of deploying components to all agents.

For example, if your network is segmented by location, and the network link between segments experiences a heavy traffic load, Trend Micro recommends allowing at least one Security Agent on each segment to act as an Update Agent.

## Dedicated Server

When selecting the client to host the WFBS server, consider the following:

- The CPU load the client handles
- If the client performs other functions

If the target client has other functions, choose another client that does not run critical or resource-intensive applications.

## Compatibility Issues

This section explains compatibility issues that may arise with certain third-party applications. Always refer to the documentation of all third-party applications that are installed on the same computer on which you will install the Security Server and other Worry Free components.

### **Other Endpoint Security Software**

Before installing the Security Server, Trend Micro recommends manually removing other endpoint security software from the target computer as this may block the installation or influence the Security Server's performance later after installation.

### **Security Applications in Windows SBS and EBS 2008**

WFBS is compatible with both Windows Small Business Server (SBS) 2008 and Windows Essential Business Server (EBS) 2008. However, some security applications that are either installed with or managed through these operating systems may conflict with WFBS. For this reason, you may need to remove these security applications.

### **Messaging Security Agent and Forefront**

The Messaging Security Agent cannot be installed on Microsoft Exchange servers that have Forefront (Microsoft Forefront Security for Exchange Server) installed. Uninstall Forefront and ensure that the Microsoft Exchange Information Store service is started before installing the Messaging Security Agent.

### **Security Agents and OneCare**

Although the Security Server can be installed with Microsoft Windows Live™ OneCare for Server, the Security Agent cannot be installed with the OneCare client. The Security Agent installer will automatically remove OneCare from clients.

### **Databases**

Scanning databases may decrease the performance of applications that access the databases. Trend Micro recommends excluding databases and their backup folders from Real-time Scan. If you need to scan a database, perform a Manual Scan or schedule a scan during off-peak hours to minimize the impact.

## Other Firewall Applications

Trend Micro recommends removing or disabling any other firewall applications prior to installing the WFBS firewall, including:

- Windows Internet Connection Firewall (ICF)
- Windows Firewall (WF)

However, if you want to run ICF or any other third-party firewall, add the Trend Micro Security Server listening ports to the firewall exception list (see *WFBS Ports on page 2-7* for information on listening ports and refer to your firewall documentation for details on how to configure exception lists).

## WFBS Ports

WFBS uses the following ports:

- **Server listening port (HTTP port):** Used to access the Security Server. By default, WFBS uses one of the following:
  - **IIS server default website:** The same port number as your HTTP server's TCP port.
  - **IIS server virtual website:** 8059
  - **Apache server:** 8059
- **Client listening port:** A randomly generated port number through which the Security Agent and Messaging Security Agent receive commands from the Security Server.

You can modify the listening ports only during the installation.



### WARNING!

Today's cyber criminals use HTTP and direct their attacks at ports 80 and/or 8080 – commonly used in most organizations as the default Transmission Control Protocol (TCP) ports for HTTP communications. If your organization is currently using one of these ports as the HTTP port, Trend Micro recommends using another port number.

---

**Note**

To find out which port your Security Agents are using to connect to the Scan Server, open SSCFG.ini in the folder where the server is installed.

- **Scan Server ports:** Used by the Scan Server to communicate with Security Agents for scan queries.

**TABLE 2-1. Scan Server Ports**

PORT TYPE	IIS DEFAULT	IIS VIRTUAL	PRE-INSTALLED APACHE	NEW APACHE INSTALLATION
Non-SSL port	Non-SSL port on web server	First open port in range 8082 to 65536	Non-SSL port on web server	Non-SSL port on web server
SSL port Using SSL	SSL port on web server	First open port in range 4345 to 65536	N/A	SSL port on web server
SSL port Not using SSL	First open port in range 4345 to 65536	First open port in range 4345 to 65536	N/A	First open port in range 4345 to 65536

- **Trend Micro Security (for Mac) Communication port:** Used by the Trend Micro Security (for Mac) server to communicate with Mac clients. The default is port 61617.
- **SMTP port:** Used by the Security Server to send reports and notifications to administrators through email. The default is port 25.
- **Proxy port:** Used for connections through a proxy server.

## Installation Checklist

Setup prompts you for the following information when you install the Security Server.

**TABLE 2-2. Installation Checklist**

INFORMATION	DEFAULT VALUES	YOUR VALUE
<b>Security Server (including Scan Server)</b>		
Activation Code	Provided by Trend Micro	
Installation path	One of the following (depending on the operating system): <ul style="list-style-type: none"> <li>• C:\Program Files \TrendMicro\Security Server</li> <li>• C:\Program Files (x86)\Trend Micro \Security Server</li> </ul>	
Scan Server Database path	Same as Security Server installation path (customizable)	
IPv4/IPv6 address	User-defined	
Fully Qualified Domain Name (FQDN)	User-defined	
NetBIOS (host) name	User-defined	
Web server	Choose one: <ul style="list-style-type: none"> <li>• Apache</li> <li>• IIS (default website)</li> <li>• IIS virtual website)</li> </ul>	
Listening port (HTTP)	8059	
Listening port (HTTPS)	4343	
Web console password	User-defined	

INFORMATION	DEFAULT VALUES	YOUR VALUE
Security Agent uninstallation/unload password	User-defined	
<b>(Optional) SMTP settings for Security Server reports and notifications sent through email</b>		
IPv4/IPv6 address	User-defined	
Fully Qualified Domain Name (FQDN)	User-defined	
NetBIOS (host) name	User-defined	
Port	25	
Recipients	User-defined	
<b>(Optional) Proxy settings for Security Server connection to Trend Micro hosted services</b>		
IPv4/IPv6 address	User-defined	
Fully Qualified Domain Name (FQDN)	User-defined	
NetBIOS (host) name	User-defined	
Authentication user name	User-defined	
Authentication password	User-defined	
<b>Security Agents</b>		
Listening port	Randomly generated by the installation program	

INFORMATION	DEFAULT VALUES	YOUR VALUE
Installation path	One of the following (depending on the operating system): <ul style="list-style-type: none"> <li>• C:\Program Files \TrendMicro\Security Agent</li> <li>• C:\Program Files (x86)\Trend Micro \Security Agent</li> </ul>	
<b>(Optional) Proxy authentication for Security Agent features (Behavior Monitoring, Web Reputation, and Smart Scan)</b>		
<div style="display: flex; align-items: center;">  <div> <p><b>Note</b></p> <p>Security Agents use the proxy settings configured in Internet Explorer.</p> </div> </div>		
Authentication user name	User-defined	
Authentication password	User-defined	
<b>(Optional) Messaging Security Agents</b>		
IPv4/IPv6 address of Microsoft Exchange Server	User-defined	
Fully Qualified Domain Name (FQDN) of Microsoft Exchange Server	User-defined	
NetBIOS (host) name of Microsoft Exchange Server	User-defined	
Domain administrator account and password to log on to Microsoft Exchange Server	User-defined	

INFORMATION	DEFAULT VALUES	YOUR VALUE
Listening Port	16372	
Installation path	One of the following (depending on the operating system): <ul style="list-style-type: none"> <li>• C:\Program Files\TrendMicro\Messaging Security Agent</li> <li>• C:\Program Files(x86)\Trend Micro\Messaging Security Agent</li> </ul>	
Temp folder (The installation program extracts the installation files to this folder)	C\$	

## Installing the Security Server

Installing the Security Server involves these phases:

PHASES	KEY TASKS
Phase 1: Starting the Security Server installation	<ul style="list-style-type: none"> <li>• Read pre-installation guidelines.</li> <li>• Launch the installation package.</li> <li>• Accept the terms of the license agreement.</li> <li>• Choose a Setup type.               <ul style="list-style-type: none"> <li>• Typical (recommended)</li> <li>• Minimal</li> <li>• Custom</li> </ul> </li> <li>• Provide your Activation Code.</li> </ul>

PHASES	KEY TASKS
Phase 2: Configuring settings according to your selected Setup type	<p>For a Typical or Minimal Installation, configure basic settings, including:</p> <ul style="list-style-type: none"> <li>• Security Server installation location</li> <li>• Administrator account passwords</li> <li>• SMTP server settings and notification recipients</li> <li>• Smart Protection Network</li> </ul>
	<p>For a Custom Installation, configure all the customizable settings, including:</p> <ul style="list-style-type: none"> <li>• Basic settings <ul style="list-style-type: none"> <li>• Security Server installation location</li> <li>• Scan Server database location</li> <li>• Whether to install the Security Agent or Messaging Security Agent on the same computer as the Security Server</li> </ul> </li> <li>• Security Server settings <ul style="list-style-type: none"> <li>• Web server</li> <li>• Administrator account password</li> <li>• SMTP server settings and notification recipients</li> <li>• Smart Protection Network</li> <li>• General proxy settings</li> </ul> </li> <li>• Security Agent settings <ul style="list-style-type: none"> <li>• Security Agent installation path</li> <li>• Security Agent features to enable</li> <li>• Proxy settings for additional services</li> </ul> </li> <li>• Messaging Security Agent settings <ul style="list-style-type: none"> <li>• Microsoft Exchange server settings</li> <li>• Messaging Security Agent installation location</li> </ul> </li> </ul>

PHASES	KEY TASKS
Phase 3: Installation Process	Wait for the installation to finish and then close Setup.

## Phase 1: Starting the Security Server Installation

### Before you begin

- Log on to the computer using an account with either domain or local administrator privileges.
- Close any running applications before installing WFBS. If you install while other applications are running, the installation process may take longer to complete.
- Make sure that you do not install the Security Server on a computer that is running applications that might lock IIS. This could prevent successful installation. See your IIS documentation for more information.
- Installing the Trend Micro Security Server does not require you to restart the computer. After completing the installation, immediately configure settings on the web console and then proceed to install the Security Agent to clients.

## Launch the Installation Package

Double-click the installation package (.exe file).



The installation files will be extracted to the same directory where the .exe file is located. To change the path, click **Browse** and then locate the directory.

When you click **Start**, Setup begins to extract the files. The extraction status displays in the status bar at the bottom of the screen. When extraction is complete, the Welcome screen displays.



## License Agreement



Read the license agreement. If you agree with the terms, select **I accept the terms of the license agreement**.

## Setup Type



Choose one of the following options:

### **Typical Installation (Recommended)**

This method is suitable on a Security Server managing up to 100 agents.

During a Typical Installation:

- The following features are automatically enabled after the installation:
  - Antivirus/Anti-spyware
  - Behavior Monitoring (only on desktop platforms, such as Windows 7)

- Web Reputation
- URL Filtering
- Smart Scan

**Note**

Security Agents must meet the minimum system requirements to run smart scan. For a list of requirements, visit <http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx>.

---

- If not present, the Security Agent is automatically installed on the same computer as the Security Server.

**Note**

Install the Security Agent to other clients in the network and manage them from the web console. See the Administrator's Guide for details on the different Security Agent installation methods.

---

- If another endpoint security software is installed on the computer, Setup first uninstalls the software and then installs the Security Agent.

**Note**

Some endpoint security software can only be detected but not uninstalled. In this case, manually uninstall the software first.

Visit the following website for a list of endpoint security software that can be uninstalled or detected only but not uninstalled:

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

---

## Minimal Installation

During a Minimal Installation:

- Only the Antivirus/Anti-spyware feature is enabled after the installation.
- If not present, the Security Agent is automatically installed on the same computer as the Security Server.



**Note**

Install the Security Agent to other clients in the network and manage them from the web console. See the Administrator's Guide for details on the different Security Agent installation methods.

---

- If another endpoint security software is installed on the computer, Setup first uninstalls the software and then installs the Security Agent.
- 



**Note**

Some endpoint security software can only be detected but not uninstalled. In this case, manually uninstall the software first.

Visit the following website for a list of endpoint security software that can be uninstalled or detected only but not uninstalled:

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

---

## Custom Installation

With Custom Installation, you have the added flexibility of configuring settings for the Security Server and agents according to your network security strategy. This method is suitable if the Security Server will manage a large number of agents.

During a Custom Installation, the following settings are **optional**:

- If not present, install the Security Agent on the same computer as the Security Server.
- 



**Note**

Install the Security Agent to other clients in the network and manage them from the web console. See the Administrator's Guide for details on the different Security Agent installation methods.

---

- If another endpoint security software is installed on the computer, Setup first uninstalls the software and then installs the Security Agent.

**Note**

Some endpoint security software can only be detected but not uninstalled. In this case, manually uninstall the software first.

Visit the following website for a list of endpoint security software that can be uninstalled or detected only but not uninstalled:

<http://esupport.trendmicro.com/solution/en-US/1060980.aspx>

- Install the Messaging Security Agent on the same computer as the Security Server (if a Microsoft Exchange server exists) or to remote clients.

## Product Activation

The screenshot shows a dialog box titled "Trend Micro Worry-Free Business Security Advanced" with a sub-header "Product Activation". The text inside reads: "Activation is required to use Worry-Free Business Security." followed by the Trend Micro logo. Below this, it says "Please enter the activation code to receive full protection. Leaving this field blank will install a 30-day trial version." There is a text input field labeled "Activation Code:" with a placeholder of 20 diamond symbols. Below the field is a "Register Online" button. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The text "InstallShield" is visible in the bottom left corner of the dialog.

Type the Activation Code in the **Activation Code** field.

If you do not have an Activation Code, you may not have registered your copy of WFBS yet. Click the **Register Online** button to open a new browser window. Follow the instructions on the Registration screen. Alternatively, click **Next** to install the evaluation version. If you upgrade to the full version before the 30-day evaluation period ends, all your program settings will remain.

## Setup Overview



The Setup Overview screen shows the components that you need to configure in order to install the Trend Micro Security Server, the Security Agent, or the Messaging Security Agent.

After you click **Next**:

- If you chose Typical/Minimal Installation, proceed to:
  - *Configuring Settings for a Typical or Minimal Installation on page 2-23*
  - *Phase 3: Installation Process on page 2-50*
- If you chose Custom Installation, proceed to:
  - *Configuring Settings for a Custom Installation on page 2-28*
  - *Phase 3: Installation Process on page 2-50*

## Phase 2: Configuring Settings According to Setup Type

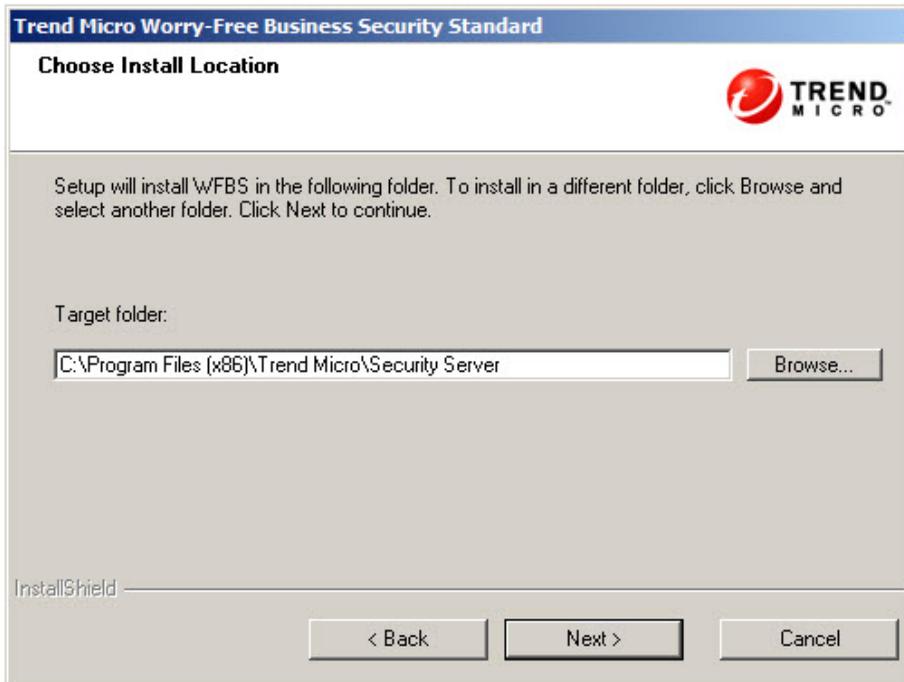
The settings you need to configure in Phase 2 depend on the Setup type you chose in Phase 1.

- *Configuring Settings for a Typical or Minimal Installation on page 2-23*
- *Configuring Settings for a Custom Installation on page 2-28*

## Configuring Settings for a Typical or Minimal Installation

If you are performing a Typical or Minimal Installation, the following screens appear sequentially:

## Installation Location



The default WFBS install folder is C:\Program Files\Trend Micro\Security Server or C:\Program Files (x86)\Trend Micro\Security Server. Click **Browse** if you want to install WFBS in another folder.

## Administrator Account Password

**Trend Micro Worry-Free Business Security Advanced**

**Administrator Account Password**

Type a password and confirm that password in the field provided.

Protect the Security Server Web console and clients with passwords to prevent unauthorized users from modifying your settings or removing your clients.

**Security Server Web console:**

Password:

Confirm Password:

**Security Agents:**

Same as above

Password:

Confirm Password:

InstallShield

< Back    Next >    Cancel

Specify different passwords for the Security Server web console and the Security Agent.

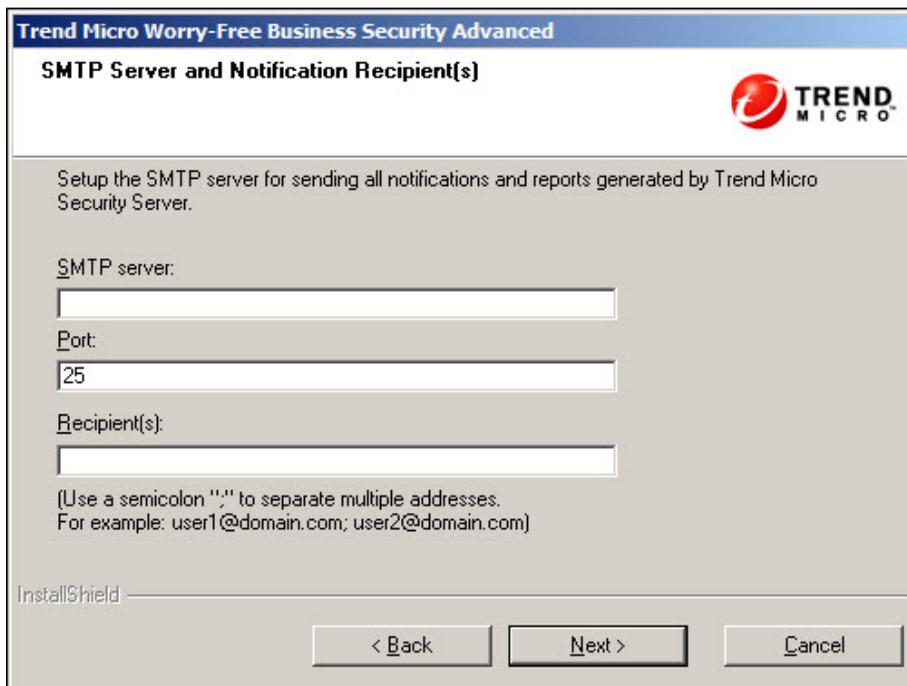
- **Security Server Web Console:** Required to log on the Web Console
- **Security Agents:** Required to uninstall or unload Security Agents from clients



### Note

The password field holds 1 – 24 characters and is case sensitive.

## SMTP Server and Notification Recipients



The screenshot shows a configuration window titled "Trend Micro Worry-Free Business Security Advanced" with a subtitle "SMTP Server and Notification Recipient(s)". The window includes the Trend Micro logo and a brief instruction: "Setup the SMTP server for sending all notifications and reports generated by Trend Micro Security Server." Below this, there are three input fields: "SMTP server:" (empty), "Port:" (containing "25"), and "Recipient(s):" (empty). A note below the fields states: "(Use a semicolon ';' to separate multiple addresses. For example: user1@domain.com; user2@domain.com)". At the bottom left, it says "InstallShield" and at the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Specify the following information:

- **SMTP server:** The IP address of your email server



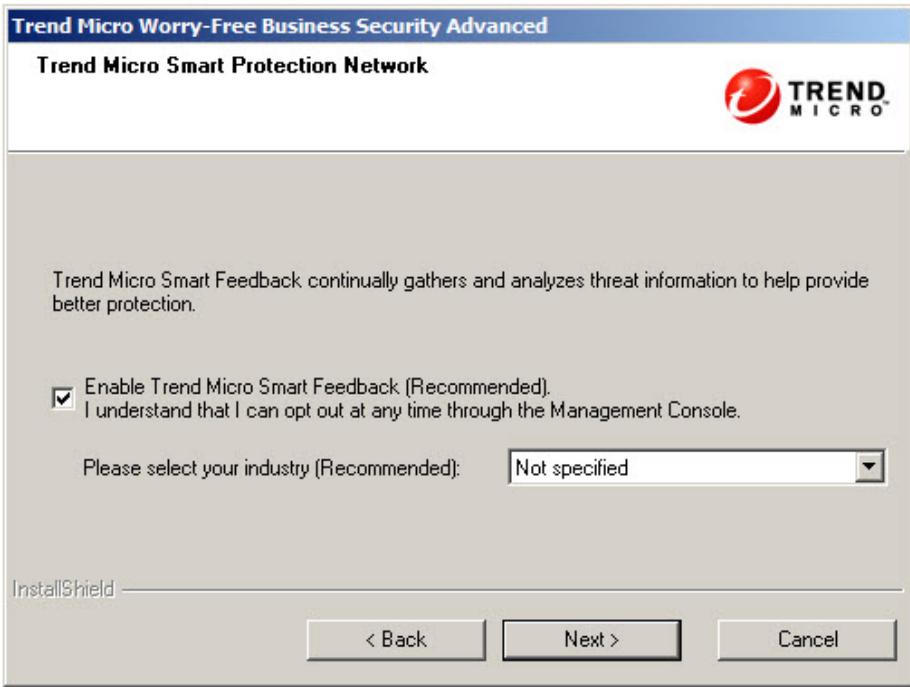
If the SMTP server is on the same computer as WFBS and uses port 25, the installation program detects the name of the SMTP server and updates the SMTP Server and Port fields.

- **Port:** The port that the SMTP server uses for communications

- **Recipient(s):** The email address(es) that the SMTP server uses to send alert notifications. You can enter multiple email addresses when more than one person needs to receive notifications

Refer to your ISP mail server settings. If you do not know these settings, proceed with the next step. You can update the SMTP settings after installation. Refer to the Administrator's Guide for instructions.

## Smart Protection Network



The screenshot shows a dialog box titled "Trend Micro Worry-Free Business Security Advanced" with a sub-header "Trend Micro Smart Protection Network". The Trend Micro logo is in the top right corner. The main text reads: "Trend Micro Smart Feedback continually gathers and analyzes threat information to help provide better protection." Below this is a checked checkbox labeled "Enable Trend Micro Smart Feedback (Recommended)." with a note: "I understand that I can opt out at any time through the Management Console." There is a dropdown menu for "Please select your industry (Recommended):" currently set to "Not specified". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog.

Choose whether you want to participate in the Trend Micro Smart Protection Network feedback program.

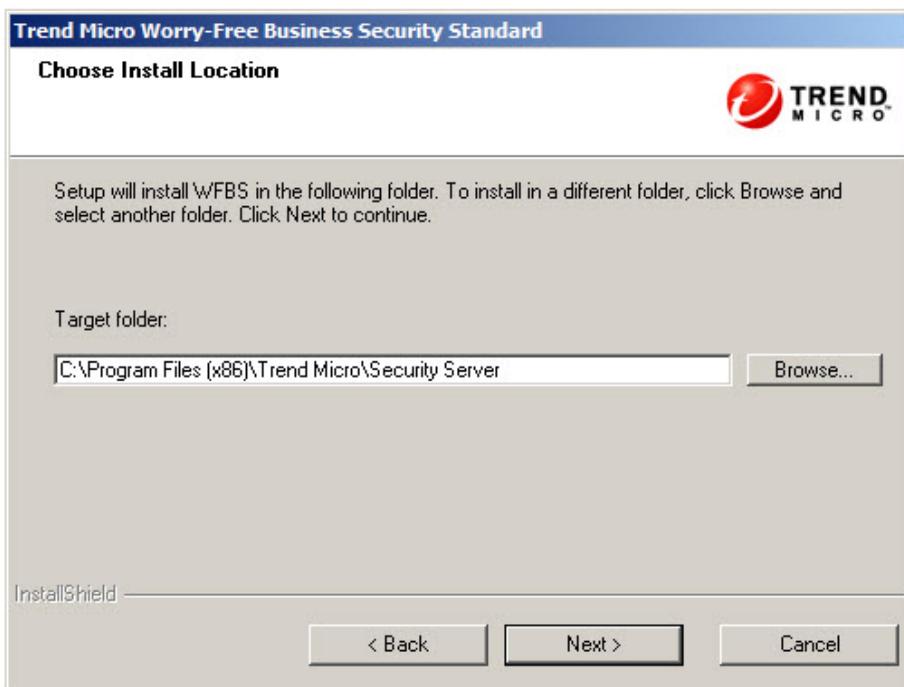
This optional feature provides feedback to Trend Micro about malware infections. Trend Micro recommends leaving the default value enabled as it uses WFBS feedback data

across the world to increase the effectiveness of its anti-malware solutions. You can choose to cancel participation through the web console later.

## Configuring Settings for a Custom Installation

If you are performing a Custom Installation, the following screens appear sequentially:

### Installation Location



The default WFBS install folder is C:\Program Files\Trend Micro\Security Server or C:\Program Files (x86)\Trend Micro\Security Server. Click **Browse** if you want to install WFBS in another folder.

## Scan Server Database Location

The screenshot shows a Windows-style dialog box titled "Trend Micro Worry-Free Business Security Advanced" with a blue header. Below the header, the title bar reads "Choose Smart Scan Server Database Location". The Trend Micro logo is in the top right corner. The main text area contains the following instructions: "By default, Setup will store the Scan Server database to the same folder as the Security Server." and "Select 'Specify a different location' only if the Security Server computer has another disk drive with at least 3GB of free disk space. Specify an absolute path (mapped drives and UNC paths are not accepted).". There are two radio button options: "Use install location" (which is selected) and "Specify a different location:". Below the "Use install location" option is a text box containing "C:\Program Files\Trend Micro\Security Server". Below the "Specify a different location:" option is another text box containing "C:\Program Files\Trend Micro\Security Server" and a "Browse..." button. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog area.

Select **Use install location** to store the Scan Server database to the same folder as the Security Server or select **Specify a different location** and type the absolute path to another location on the Security Server. It is not possible to specify a mapped drive or UNC path.

## Select Components



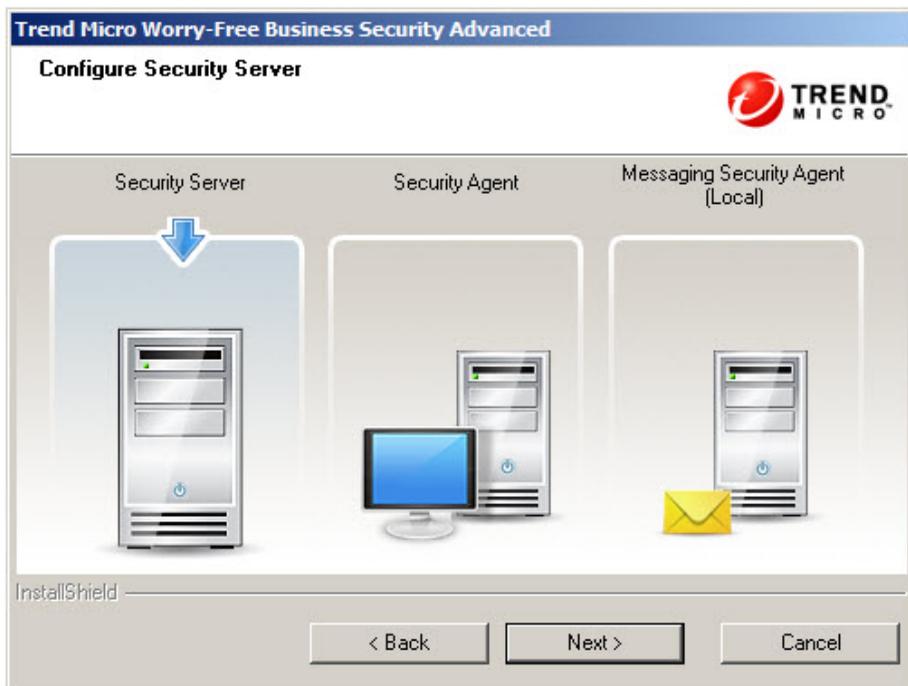
Select the components that you want to install on the target computer:

- **Security Server** (Required): The Security Server hosts the centralized web console
- **Security Agent** (Optional): The agent that protects desktops and servers
- **Messaging Security Agent** (Optional): When installing the Security Server on a computer that has a Microsoft Exchange server installed on the same computer, Setup prompts you to install a local Messaging Security Agent (Advanced only).
- **Remote Messaging Security Agent** (optional): When installing the Security Server on a computer that cannot detect the existence of local Microsoft Exchange servers, Setup prompts you to install the remote Messaging Security Agent to remote servers (Advanced only).

**Note**

If there is an Exchange server on the same computer to which you are installing the Security Server, the remote Messaging Security Agent will not show on the Select Components screen; only the local Messaging Security Agent will show.

## Configure Security Server



The Configure Security Server screen introduces the Security Server settings that you need to configure.

## Web Server



For a fresh installation, Setup checks if a web server exists on the target computer.

SCENARIO	RESULT	NOTES
Setup detects both IIS and Apache web servers	<ul style="list-style-type: none"><li>• For a typical or minimal installation, Setup automatically uses IIS.</li><li>• For a custom installation:<ul style="list-style-type: none"><li>• Setup automatically uses IIS if the Apache web server version is not supported (only versions 2.0.54, 2.0.55, 2.0.6x, and 2.2.22 are supported)</li><li>• You can choose either of the two web servers if the Apache web server version is supported.</li></ul></li></ul>	If the computer runs Windows Vista, 7, 8, or 8.1 Trend Micro recommends a custom installation and choosing Apache as the web server.
Setup detects only an IIS web server	<ul style="list-style-type: none"><li>• For a typical or minimal installation, Setup automatically uses IIS.</li><li>• For a custom installation, you can choose either of the two web servers. If you choose Apache, Setup automatically installs Apache version 2.2.22.</li></ul>	

SCENARIO	RESULT	NOTES
Setup detects only an Apache web server	<ul style="list-style-type: none"> <li>• Setup uses Apache if the Apache version is 2.0.54, 2.0.55, 2.0.6x, or 2.2.22.</li> <li>• Installation cannot proceed if other Apache versions exist. Consider the following actions:               <ul style="list-style-type: none"> <li>• Uninstall Apache if no application is using it.</li> <li>• Upgrade Apache to version 2.0.54, 2.0.55, 2.0.6x, or 2.2.22 if any of these versions is compatible with the applications that use Apache.</li> <li>• Choose another computer on which to install the Security Server.</li> </ul> </li> </ul>	<p>The following platforms have IIS and are supported by the Security Server:</p> <ul style="list-style-type: none"> <li>• Windows Server 2003/2003 R2</li> <li>• Windows SBS 2003/2003 R2</li> <li>• Windows Home Server</li> <li>• Windows Server 2008/2008 R2</li> <li>• Windows SBS 2008</li> <li>• Windows EBS 2008</li> <li>• Windows SBS 2011 Standard/Essentials</li> <li>• Windows Server 2012/2012 R2</li> </ul> <p>If Setup cannot detect IIS on these platforms, IIS may have been disabled (by default or by the system administrator). Enable IIS in this case.</p>
Setup detects neither web server	Setup automatically installs Apache web server 2.2.22.	

For upgrades, if Apache is currently used as web server:

- Setup automatically upgrades the Apache version to 2.2.22 if the Apache web server was installed by the WFBS 6.x/7.x/8.x Setup program.
- Setup keeps the existing Apache version if it was installed by other programs.

## Administrator Account Password

**Trend Micro Worry-Free Business Security Advanced**

**Administrator Account Password**

Type a password and confirm that password in the field provided.

Protect the Security Server Web console and clients with passwords to prevent unauthorized users from modifying your settings or removing your clients.

**Security Server Web console:**

Password:

Confirm Password:

**Security Agents:**  Same as above

Password:

Confirm Password:

InstallShield

< Back    Next >    Cancel

Specify different passwords for the Security Server web console and the Security Agent.

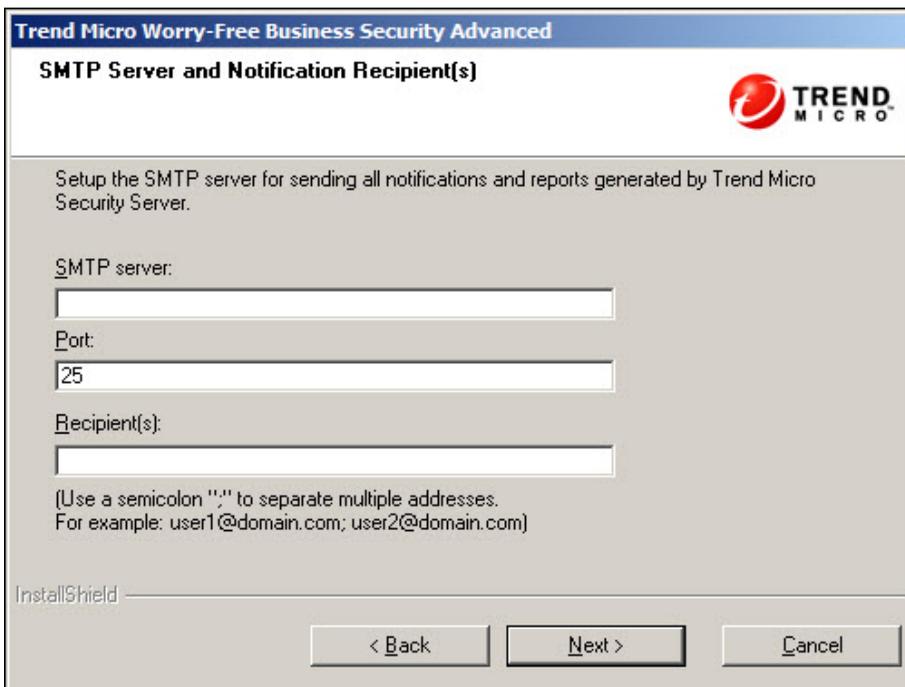
- **Security Server Web Console:** Required to log on the Web Console
- **Security Agents:** Required to uninstall or unload Security Agents from clients



### Note

The password field holds 1 – 24 characters and is case sensitive.

## SMTP Server and Notification Recipients



The screenshot shows a configuration window titled "Trend Micro Worry-Free Business Security Advanced" with a sub-header "SMTP Server and Notification Recipient(s)". The window contains the following fields and instructions:

- SMTP server:** An empty text input field.
- Port:** A text input field containing the value "25".
- Recipient(s):** An empty text input field.

Below the fields, the following instructions are provided: "(Use a semicolon ';' to separate multiple addresses. For example: user1@domain.com; user2@domain.com)". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

Specify the following information:

- **SMTP server:** The IP address of your email server



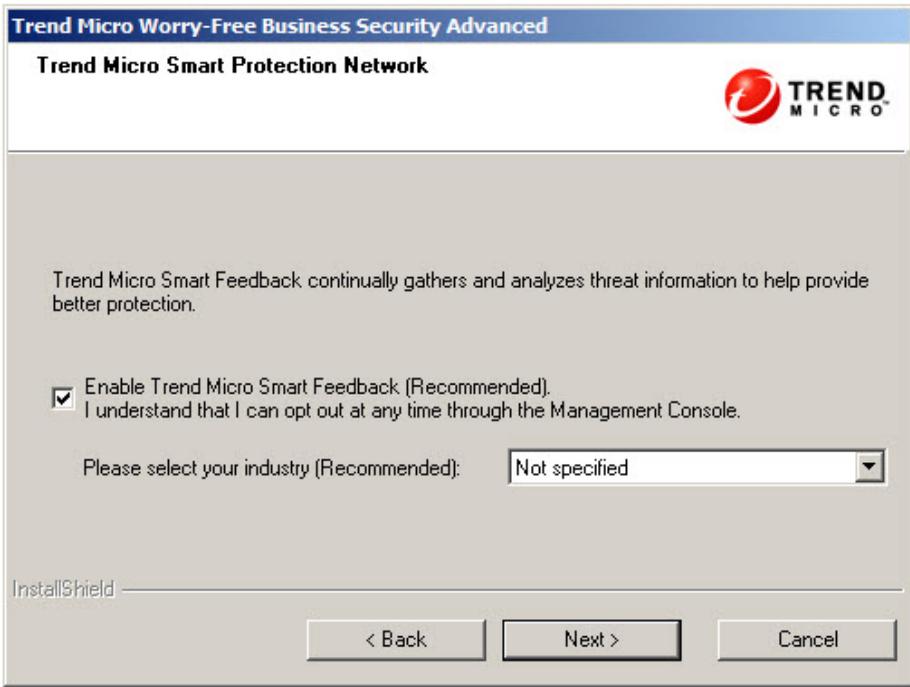
If the SMTP server is on the same computer as WFBS and uses port 25, the installation program detects the name of the SMTP server and updates the SMTP Server and Port fields.

- **Port:** The port that the SMTP server uses for communications

- **Recipient(s):** The email address(es) that the SMTP server uses to send alert notifications. You can enter multiple email addresses when more than one person needs to receive notifications

Refer to your ISP mail server settings. If you do not know these settings, proceed with the next step. You can update the SMTP settings after installation. Refer to the Administrator's Guide for instructions.

## Smart Protection Network



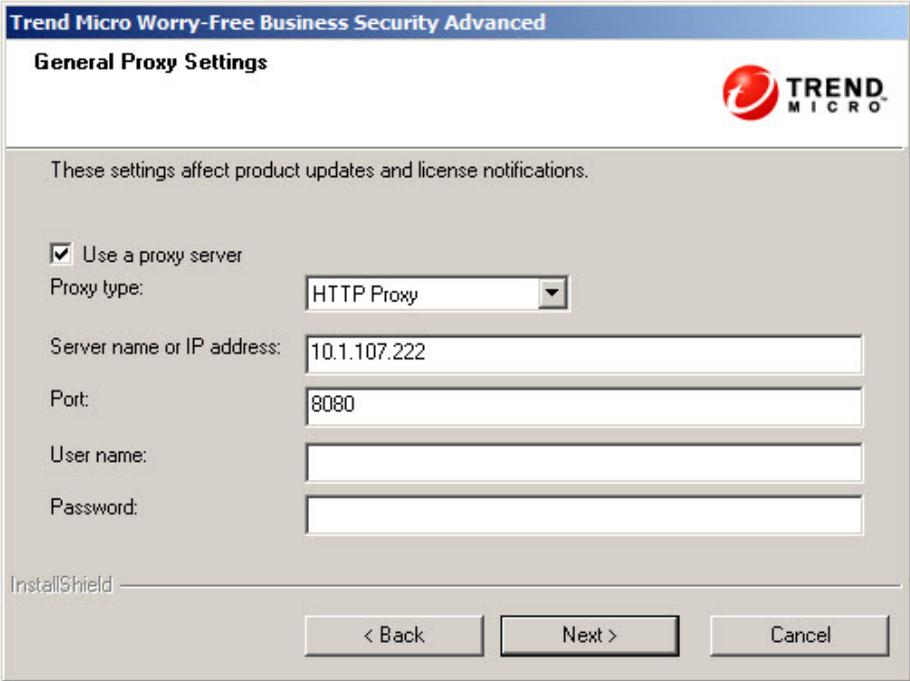
The screenshot shows a dialog box titled "Trend Micro Worry-Free Business Security Advanced" with a sub-header "Trend Micro Smart Protection Network". The Trend Micro logo is in the top right. The main text reads: "Trend Micro Smart Feedback continually gathers and analyzes threat information to help provide better protection." Below this is a checked checkbox labeled "Enable Trend Micro Smart Feedback (Recommended)." with a note: "I understand that I can opt out at any time through the Management Console." There is a label "Please select your industry (Recommended):" followed by a dropdown menu currently set to "Not specified". At the bottom left is the "InstallShield" logo, and at the bottom are three buttons: "< Back", "Next >", and "Cancel".

Choose whether you want to participate in the Trend Micro Smart Protection Network feedback program.

This optional feature provides feedback to Trend Micro about malware infections. Trend Micro recommends leaving the default value enabled as it uses WFBS feedback data

across the world to increase the effectiveness of its anti-malware solutions. You can choose to cancel participation through the web console later.

## General Proxy Settings



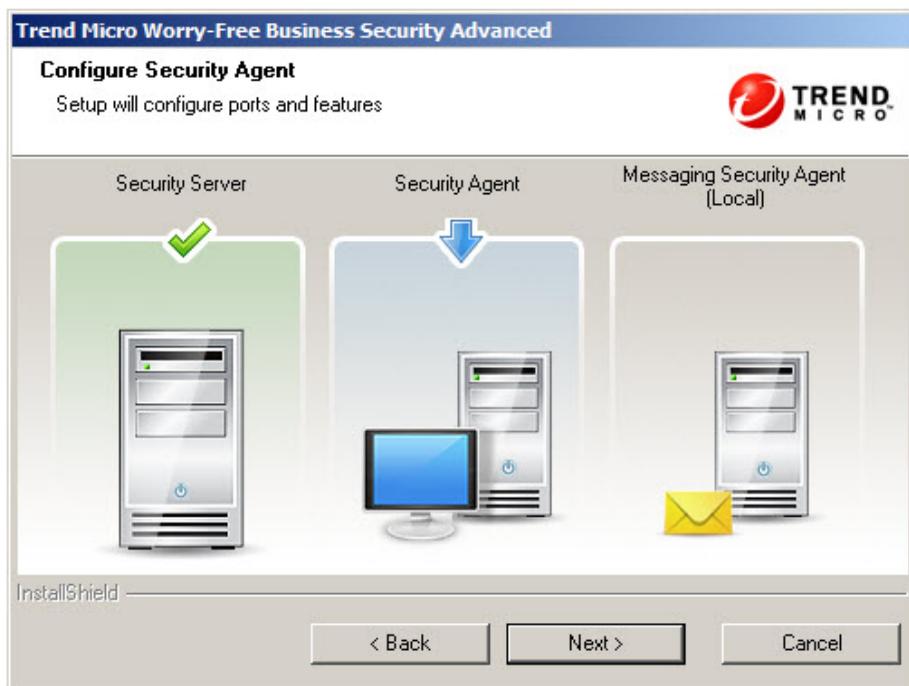
The screenshot shows a dialog box titled "Trend Micro Worry-Free Business Security Advanced" with a sub-header "General Proxy Settings". The Trend Micro logo is in the top right corner. Below the title bar, a note states: "These settings affect product updates and license notifications." The main area contains a checked checkbox labeled "Use a proxy server". Below this are several input fields: "Proxy type:" with a dropdown menu set to "HTTP Proxy"; "Server name or IP address:" with a text box containing "10.1.107.222"; "Port:" with a text box containing "8080"; "User name:" with an empty text box; and "Password:" with an empty text box. At the bottom left, the text "InstallShield" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

If a proxy server is required to access the Internet, select the **Use a proxy server** check box and provide the following information:

- **Proxy server type**
- **Server name or IP address**
- **Port**

- **User name and Password:** provide only if the proxy server requires authentication

## Configure Security Agent



The Configure Security Agent screen introduces the Security Agent settings that you need to configure.

After installing the Security Server, install the Security Agent to clients in the network. For details on the different Security Agent installation methods, see the Administrator's Guide.

## Security Agent Installation Path



Set the following items:

- **Installation Path:** The destination folder where the Security Agent files are installed
- **Security Agent Listening Port:** The port number used for Security Agent and Security Server communications

## Security Agent Settings



Configure Security Agent settings for Servers and Desktops.

- **Servers:** Security Agents running Windows server platforms (such as Windows Server 2008) will be added to the default Servers group when you first add them to the Web Console. You can enable different technologies for this group based on your particular needs
- **Desktops:** Security Agents running Windows desktop platforms (such as Windows Vista) will be added to the default Desktops group when you first add them to the Web Console. You can enable different technologies for this group based on your particular needs.

In each group, you can configure the following components:

- **Smart Scan:** Smart Scan uses a central scan server on the network to take some of the burden of the scanning of clients.
- **Antivirus and Anti-Spyware:** Scans files for malicious code as they are accessed or created
- **Firewall:** Protects clients against malware attacks and network viruses by creating a barrier between the clients and the network
- **Web Reputation:** Blocks malicious websites through the credibility of Web domains and assigning a reputation score based on several identifying factors
- **URL Filtering:** Blocks specified categories of websites (for example, pornographic, social networking) according to your company's policy
- **Behavior Monitoring:** Analyzes program behavior to proactively detect known and unknown threats
- **Trusted Program:** Allows frequently used I/O applications to be configured from the user interface
- **Device Control:** Regulates access to external storage devices and network resources

## Proxy Settings for Additional Services

The screenshot shows a dialog box titled "Trend Micro Worry-Free Business Security Advanced" with the subtitle "Proxy Settings for Additional Services". The Trend Micro logo is in the top right corner. The main text reads: "Web Reputation, Behavior Monitoring, and Smart Scanning services use the proxy server address and port used by Internet Explorer on client computers. Provide logon credentials if the proxy server requires authentication." Below this is a checked checkbox labeled "Use the credentials I specified for the general proxy settings". Underneath are two text input fields labeled "User name:" and "Password:". At the bottom left is the "InstallShield" logo, and at the bottom right are three buttons: "< Back", "Next >", and "Cancel".

The **Smart Scan**, **Web Reputation**, and **Behavior Monitoring** services use the proxy server address and port used by Internet Explorer on client computers. If that proxy server requires authentication, use this screen to specify logon credentials.

## Configure Messaging Security Agent

Install Messaging Security Agent during the Security Server installation.

### Installation notes and reminders:

- You do not need to stop or start Microsoft Exchange services before or after the installation.

- If information from a previous Messaging Security Agent installation exists on the client, you will be unable to install Messaging Security Agent successfully. Use the Windows Installer Cleanup Utility to clean up remnants of the previous installation. To download the Windows Installer Cleanup Utility, visit:  
<http://support.microsoft.com/kb/290301/en-us>
- If you are installing the Messaging Security Agent on a server that is running lockdown tools, remove the lockdown tool so that it does not disable the IIS service and causes the installation to fail.
- The Messaging Security Agent can also be installed from the web console after the installation of the Security Server. For details, see the Administrator's Guide.

Setup prompts you to install the Messaging Security Agent at one of the following points:

- When installing the Security Server on a computer that has Microsoft Exchange server installed on the same computer, Setup prompts you to install a **local** Messaging Security Agent.



- When installing the Security Server on a computer that cannot detect the existence of local Microsoft Exchange servers, Setup prompts you to install the **remote** Messaging Security Agent to remote servers.



## Install Messaging Security Agent

**Trend Micro Worry-Free Business Security Advanced**

**Install Messaging Security Agent**

You can also install Messaging Security Agent from the management console. You must specify a Domain Administrator account (Domain\Account) to that Exchange server.

No, I have finished the Messaging protection installation.
   
 Yes, I would like to install Messaging protection to the following server:

Exchange Server:

**Domain Administrator Account**

Account:

Password:

InstallShield

< Back    Next >    Cancel

Provide the following information:

- **Exchange Server**



### Note

The installation program will automatically detect the name of the local Exchange server and fill in the Exchange Server field if the Exchange server is on the same computer as the Security Server. If you have an Exchange Server installed on same computer, but the Exchange Server Name is not automatically filled in, check if the environment meets the Messaging Security Agent system requirements.

- **Domain Administrator Account**

- **Password**

**Note**

The installer may be unable to pass passwords with special, non-alphanumeric characters to the Exchange Server computer. This will prevent installation of the Messaging Security Agent. To work around this issue, either temporarily change the password to the built-in domain administrator account or install the Messaging Security Agent directly on the Microsoft Exchange server.

## Messaging Security Agent Settings

The screenshot shows the 'Messaging Security Agent Settings' dialog box from the Trend Micro Worry-Free Business Security Advanced installer. The dialog has a blue header with the product name and the Trend Micro logo. It contains two text input fields: 'Target folder:' with the path 'C:\Program Files\Trend Micro\Messaging Security Agent' and 'Temp folder:' with 'C\$'. Below these fields is a note: 'The installation files will be copied to the specified share folder on the computer that will install MSA'. Under the 'Spam Management' section, there are two radio button options: 'End User Quarantine' (unselected) and 'Outlook Junk E-mail folder' (selected). At the bottom, there is an 'InstallShield' label and three buttons: '< Back', 'Next >', and 'Cancel'.

Configure the following:

- **Target Folder:** The folder where the Messaging Security Agent files are installed
- **Temp Folder:** The folder where Setup extracts the installation files
- **End User Quarantine:** If selected, WFBS creates a separate spam folder on Microsoft Outlook in addition to the Junk E-mail folder
- **Outlook Junk Email folder:** If selected, WFBS stores spam mail into this folder. Since Microsoft Outlook typically moves spam mail in the End User Quarantine (EUQ) folder to the Junk E-mail folder, Trend Micro recommends selecting this option.

**Note**

The option to select between EUQ and the Junk E-mail folder is only available if the computer is running Exchange Server 2003. On Exchange Server 2007 and 2010, the EUQ option is disabled by default.

---

After you click **Next**, the program begins installing the Messaging Security Agent.

After installing a Messaging Security Agent remotely, repeat the agent installation process to install Messaging Security Agents remotely to other Microsoft Exchange servers.

## Phase 3: Installation Process

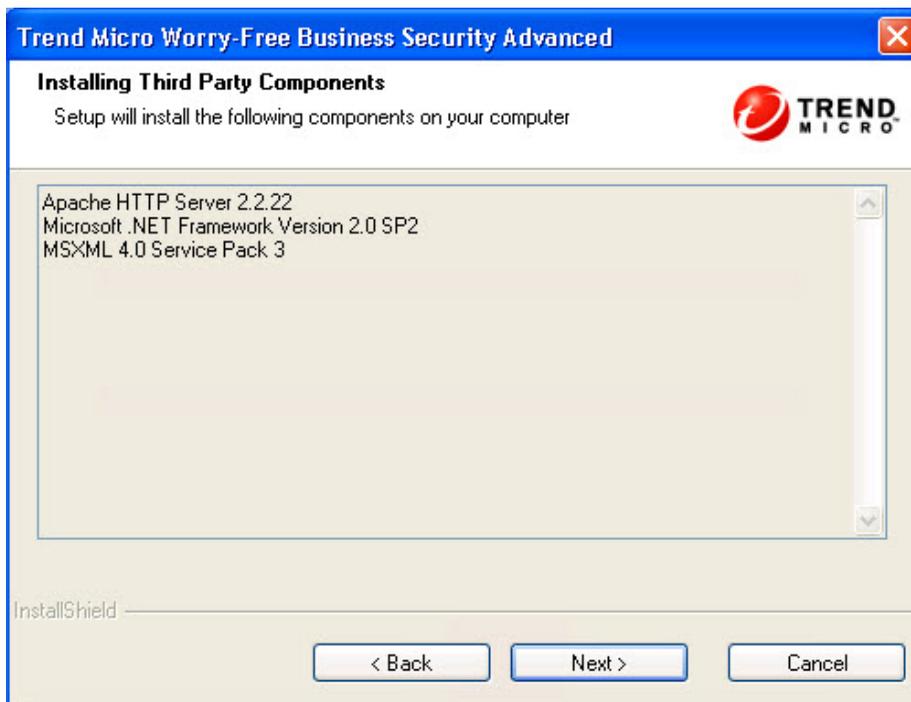
### Start Copying Files



The Start Copying Files screen shows a summary of all parameters that will be used during the installation of WFBS.

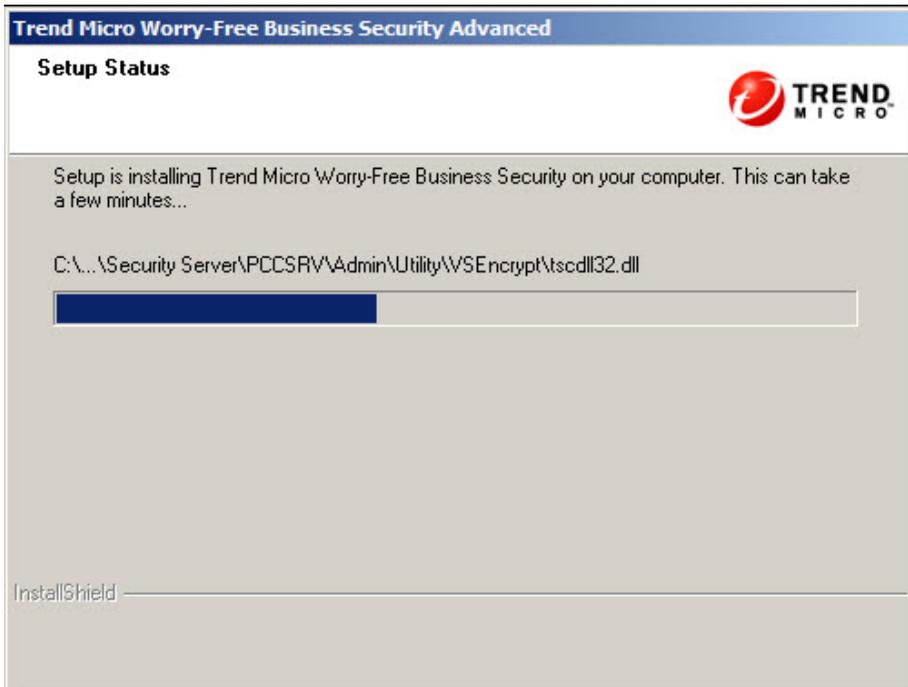
Click **Back** if you wish to verify previous installation settings, or click **Next** to proceed with the actual installation.

## Install Third Party Components



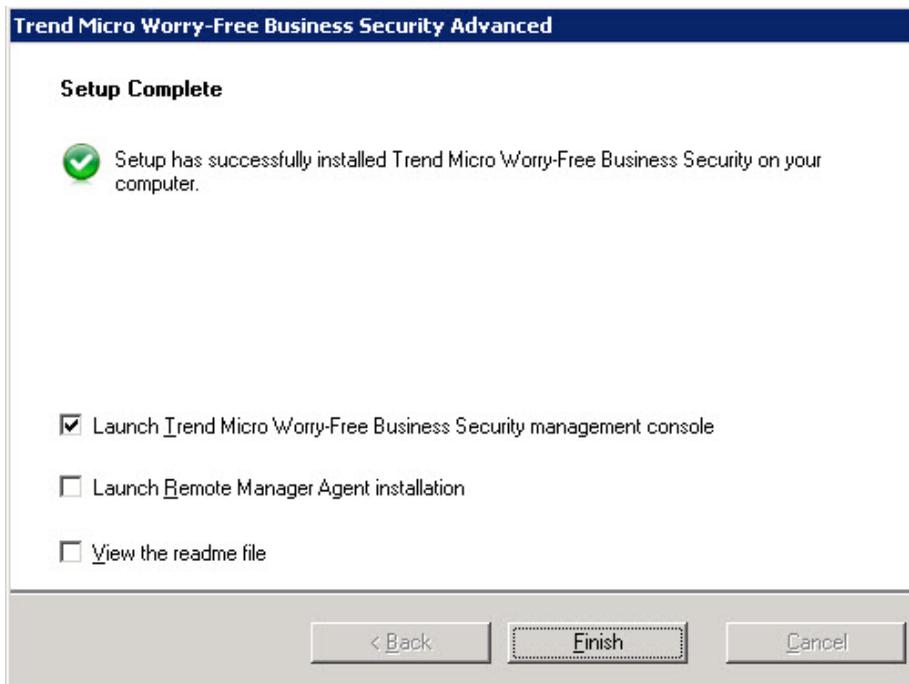
This screen informs you which third party components will be installed. Click **Next** to start installing the selected components.

## Setup Status



The entire installation process may take some time to complete. During the installation, a status screen will show the progress being made.

## Setup Complete



Optionally select the check boxes to:

- Open the web-based management console (selected by default)
- Install Remote Manager Agent (See the *Administrator's Guide* for the procedure)
- View the readme file

Click **Finish** to close the install procedure.

## Installing Several Security Servers Using Silent Installation

Use Silent installation to help you run multiple identical installations on separate networks. You can record the installation settings in one Setup Wizard session and then use these settings to generate automated installations.

### Recording an Installation Session

#### Procedure

1. Download and extract the WFBS files on your hard disk. When the Setup Wizard starts with collecting installation settings, click **Cancel** > **Yes** > **Finish**.

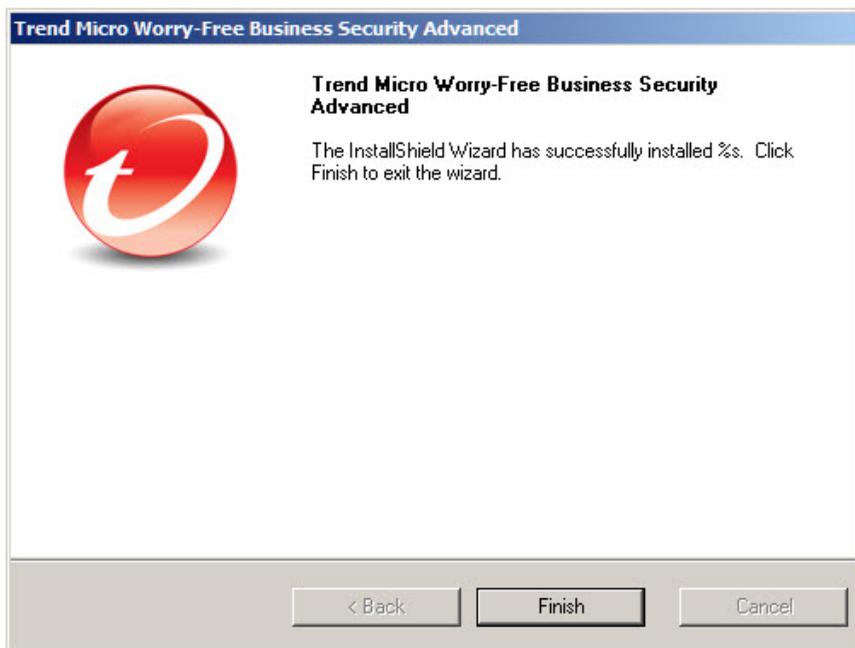


2. In command prompt mode, navigate to the directory where the extracted WFBS setup files are located, for example: `C:\Extract\WFBS\CSM`

3. At the prompt, type `Setup.exe /r /f1"c:\silent-install.iss"` and click **Enter**.

The Setup Wizard will start again. Your input will be recorded in the silent-install.iss file on drive C.

4. Follow the instructions on you screen. The instructions are the same as described in *Installing the Security Server on page 2-12*.
5. At the end of the recording session the following confirmation screen appears. Click **Finish** to end the recording session and return to the command prompt mode.



## Starting the Silent Installation

---

### Procedure

1. In command prompt mode, navigate to the directory where the extracted WFBS setup files are located, for example: `C:\Extract\WFBS\CSM`
2. At the prompt, type `Setup.exe /s /f1"c:\silent-install.iss"` and click **Enter**.

The silent WFBS installation will automatically start and will take the same amount of time as a normal installation.

During Silent installation, no progress indicators will be shown on your screen.

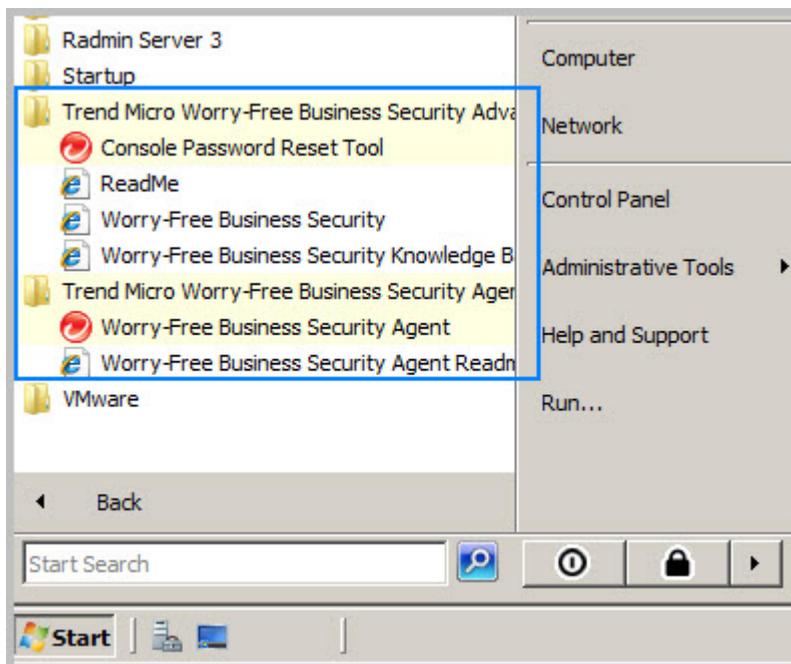
3. To verify that the installation is successful, open the `c:\setup.log` file. If `ResultCode=0`, the installation was successful.
  4. Repeat steps 1 to 3 on all other computers in your network.
- 

## Verifying the Installation

---

### Procedure

- Click **Start > All Programs** to see if the Security Server and the Security Agent appear in the list.



- Click **Start > Control Panel > Programs > Uninstall a Program** to see if the WFBS program and the Security Agent appear in the list.
- Log on to the Management Console with the server URL: `https://{server_name}:{port number}/SMB`



#### Note

If you are not using a Security Socket Layer (SSL), type `http` instead of `https`.



## Chapter 3

# Upgrading the Security Server and Agents

This chapter provides information you will need to understand to upgrade the Security Server and Agents.

## Installation and Upgrade Requirements

Visit the following website for a complete list of installation and upgrade requirements:

<http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx>

## Upgrade Considerations

Consider the following when upgrading the Security Server and agents.

- *IPv6 Requirements for Upgrades on page 3-2*
- *Upgrade Best Practices on page 3-3*

## IPv6 Requirements for Upgrades

The IPv6 requirements for the Security Server are as follows:

- The Security Server to be upgraded must be installed on Windows Server 2008, SBS 2008/2011, 7, and Vista. Security Servers on Windows XP, Server 2003, and SBS 2003 cannot be upgraded because these operating systems only support IPv6 addressing partially.
- The Security Server must already be using an IIS web server. Apache web server does not support IPv6 addressing.
- Assign an IPv6 address to the Security Server. In addition, the server must be identified by its host name, preferably its Fully Qualified Domain Name (FQDN). If the server is identified by its IPv6 address, all clients currently managed by the server will lose connection with the server. If the server is identified by its IPv4 address, it will not be able to deploy the agent to pure IPv6 clients.
- Verify that the Security Server host machine's IPv6 or IPv4 address can be retrieved using, for example, the “ping” or “nslookup” command.

## Upgrade Best Practices

You can preserve your client settings when you upgrade to the newest version of WFBS. To ensure that you can easily restore your existing settings if the upgrade is unsuccessful, Trend Micro recommends the following:

- Backing up the Security Server database
- Deleting all log files from the Security Server

## Backing Up the Security Server Database

---

### Procedure

1. Stop the Trend Micro Security Server Master Service.
  2. In Windows Explorer, go to the Security Server folder and copy the contents of `\PCCSRV\HTTPDB` to another location (for example, to a different folder on the same server, to another computer, or to a removable drive).
- 

## Deleting Log Files from the Security Server

---

### Procedure

1. Go to **Reports > Maintenance > Manual Log Deletion**.
  2. Set **Delete Logs Older Than** to 0 for a log type.
  3. Click **Delete**.
  4. Repeat steps 2 to 3 for all log types.
- 

## Previous Version Upgrades

This product version supports upgrades from any of the following WFBS or WFBS-Advanced versions:

- 9.0
- 8.x (8.0 and 8.0 SP1)
- 7.x (7.0 and 7.0 SP1)
- 6.x (6.0, SP1, SP2, and SP3)

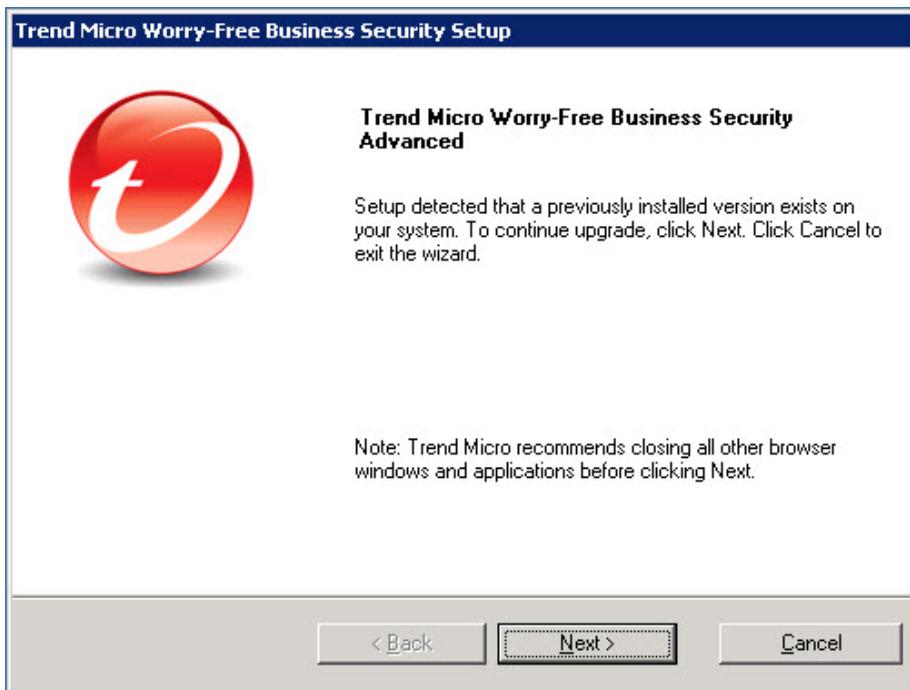
This product version does not support upgrades from any of the following:

- WFBS or WFBS-Advanced 5.x
- All upgrades that supported Windows 2000
- Client/Server Messaging Security 3.6 (except for Japanese version)
- Client/Server/Messaging Security 3.5
- Client/Server/Messaging Security 3.0
- Client/Server Security 3.0
- Client/Server Suite 2.0
- Client/Server/Messaging Suite 2.0
- OfficeScan or ScanMail for Microsoft Exchange
- One language to another

Depending on network bandwidth and the number of agents the Security Server manages, you can stagger the agent upgrade in groups or upgrade all agents immediately after the server upgrades.

## Upgrade Method 1: Using the Installation Package to Upgrade

Obtain the installation package for this product version and then run `Setup.exe` on the Security Server computer. When Setup detects that an existing Security Server exists on the computer, it prompts you to upgrade, as shown in the following image.



Follow the on-screen instructions to upgrade the Security Server.

On one of the installation screens, choose from the following Security Agent upgrade options:

**Trend Micro Worry-Free Business Security Setup**

**Upgrading the Security Agents**



After completing the Security Server upgrade:

Note: All agents will upgrade even if you enable the option "Disable program upgrade and hot fix deployment" in the web console (Security Settings > {Group} > Configure > Client Privileges > Update Privileges section).

Automatically upgrade all Security Agents in your network

Allow clients to delay upgrading their Security Agent for maximum period of:

2 hours

InstallShield

< Back    Next >    Cancel

SECURITY AGENT UPGRADE OPTION	DETAILS
Automatically upgrade all Security Agents in your network	<p>If you have a small number of Security Agents, allow all agents to upgrade immediately after the Security Server upgrades.</p> <p>All agents will upgrade, even if the option <b>Disable Security Agent/program upgrade and hot fix deployment</b> is enabled on the web console, in <b>Security Settings &gt; {Group} &gt; Configure &gt; Client Privileges</b>.</p> <hr/> <p> <b>Note</b></p> <p>The option <b>Disable Security Agent/program upgrade and hot fix deployment</b> only prevents build upgrades (for example, from the Beta build to the release build) but not version upgrades. If currently enabled, this option will automatically be disabled after the upgrade. Re-enable it as required.</p>

SECURITY AGENT UPGRADE OPTION	DETAILS
<p>Allow clients to delay upgrading their Security Agent for a maximum period of __ hours</p>	<p>Select this option when upgrading a large number of Security Agents. Specify the maximum number of hours (2, 4, 8, 12, or 24 hours) to delay the upgrade.</p> <p>After the Security Server upgrades, it sends upgrade notifications to all Security Agents. Users see a popup message on their computers, prompting them to upgrade.</p>  <ul style="list-style-type: none"> <li>• If users click <b>Upgrade Now</b>, the upgrade starts immediately.</li> <li>• If users do nothing, the upgrade automatically starts 5 minutes after the message displays.</li> <li>• If users click <b>Remind Me Later</b>, the Security Agent displays the popup message every 30 minutes until the upgrade has been started, either by the user or automatically (if users do nothing or after the maximum number of hours you specified has elapsed). The maximum number of hours takes effect when the popup message first displayed and is not reset each time the user delays the upgrade or if the client computer was shut down or restarted.</li> </ul> <p>Agents that are pending upgrade still receive component updates (such as the pattern files) to keep their protection up-to-date.</p>

## Upgrade Results

- Online Security Agents upgrade immediately or after a number of hours, depending on the upgrade option you selected.
- Online Messaging Security Agents upgrade immediately.
- Offline agents upgrade when they become online.
  - For offline Messaging Security Agents, check the connection status with the Security Server.
  - For offline Security Agents, instruct users to connect to the network so that the agent can become online. For Security Agents that are offline for an extended period of time, instruct users to uninstall the agent from the client and then use a suitable agent installation method (such as Client Packager) discussed in the *Administrator's Guide* to install the agent.



### Note

All previous agent settings, except Update Agent privileges, will be retained after upgrading to this version. This means that Update Agents will revert to being Security Agents after the upgrade. Reassign them as Update Agents from the management console. Refer to <http://esupport.trendmicro.com/solution/en-US/1057531.aspx> for details.

---

## Upgrade Method 2: Move Agents to Security Server 9.0 SP1

Perform a fresh installation of the Security Server and then move agents (Security Agents and Messaging Security Agents) to this server. When you move the agents, they automatically upgrade to version 9.0 SP1.

## Part 1: Perform a Fresh Installation of Security Server 9.0 SP1

---

### Procedure

1. Perform a fresh installation of the Security Server on a computer. For details, see [Installing the Security Server on page 2-12](#).
2. Record the following Security Server 9.0 SP1 information. Specify this information on the Security Server 6.x, 7.x, 8.x, or 9.0 when moving agents.
  - Host name or IP address
  - Server listening port

The host name and listening port are found on the Security Server's Security Settings screen, above the Tasks panel.

---

## Part 2: Upgrade Agents

---

### Procedure

1. On the Security Server 6.x, 7.x, 8.x, or 9.0 web console, navigate to **Security Settings**.
2. To move Security Agents, select a group and then select the agents. To move a Messaging Security Agent, select it.



To select multiple, adjacent Security Agents, click the first agent in the range, hold down the SHIFT key, and then click the last agent in the range. To select a range of non-contiguous agents, click the first agent in the range, hold down the CTRL key, and then click the agents you want to select.

---

3. Click **Move**.

A new screen appears.

4. Type the host name and listening port of the Security Server 9.0 SP1 to which agents will move.
  5. Click **Move**.
- 

## Upgrade Results

- Online agents start to move and upgrade. After upgrading:
  - Security Agents will be grouped under the **Desktops (default)** or **Servers (default)** group in the Security Server 9.0 SP1, depending on the operating system of the client. The agent inherits the settings of its new group.
  - A Messaging Security Agent will be its own group in the Security Server 9.0 SP1 and will retain its settings.
- Offline agents upgrade when they become online.
  - For offline Messaging Security Agents, check the connection status with the Security Server.
  - For offline Security Agents, instruct users to connect to the network so that the agent can become online. For Security Agents that are offline for an extended period of time, instruct users to uninstall the agent from the client and then use a suitable agent installation method (such as Client Packager) discussed in the *Administrator's Guide* to install the agent.

## Upgrades to the Full Version or the Advanced Edition

Use the Product License screen on the web console to:

- Upgrade from the Evaluation to the Full version of the product
- Upgrade from the Standard to the Advanced Edition of the product

### Evaluation and Full Versions

When your evaluation version is about to expire, a notification message displays on the Live Status screen on the web console. You can upgrade from an evaluation version to

the fully licensed version using the Web Console. Your configuration settings will be saved. When you purchase a fully licensed version, you will receive a Registration Key or an Activation Code.

## Standard and Advanced Editions

Trend Micro offers two similar products to protect your clients and network: Worry-Free Business Security Standard and Worry-Free Business Security Advanced.

**TABLE 3-1. Product Versions**

PRODUCT VERSION	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Client-side solution	Yes	Yes
Server-side solution	Yes	Yes
Microsoft Exchange Server solution	No	Yes

You can upgrade from Worry-Free Business Security to Worry-Free Business Security Advanced by obtaining an Activation Code from Trend Micro.

## Upgrading to the Full Version or the Advanced Edition

---

### Procedure

1. On the web console, navigate to **Preferences > Product License**.
2. If you have an Activation Code, click **Enter a new code**, type it in the **New Activation Code** field, and click **Activate**.

If you do not have an Activation Code, go to the Trend Micro website at <http://olr.trendmicro.com> to register online and obtain your Activation Code.

---

# Appendix A

## Getting Help

This appendix describes how to get help, find additional information, and contact Trend Micro.

## The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro website, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

<http://esupport.trendmicro.com/en-us/business/default.aspx>

Trend Micro updates the contents of the Knowledge Base continuously and adds new solutions daily. If you are unable to find an answer, however, you can describe the problem in an email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

## Contacting Technical Support

Before contacting Trend Micro Technical Support it is recommended that you run the Case Diagnostic Tool first (See *Case Diagnostic Tool on page A-3*).

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

- Technical Support:

<http://esupport.trendmicro.com/en-us/business/pages/technical-support.aspx>

- Submit a Support Case Online:

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

- If you prefer to communicate by email message, send a query to the following address:

support@trendmicro.com

- In the United States, you can also call the following toll-free telephone number:

(877) TRENDAY, or 877-873-6328

- Trend Micro product documentation:  
<http://docs.trendmicro.com/en-us/smb.aspx>

## Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) collects necessary debugging information from a customer's product whenever problems occur. It automatically turns the product's debug status on and off and collects necessary files according to problem categories. Trend Micro uses this information to troubleshoot problems related to the product.

Run the tool on all platforms that WFBS supports. To obtain this tool and relevant documentation, contact your support provider.

## Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your client
- Amount of memory and free hard disk space on your client
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

## Contact Information

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

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

Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main) Fax: +1 (408) 257-2003

Web address: [www.trendmicro.com](http://www.trendmicro.com)

Email: [support@trendmicro.com](mailto:support@trendmicro.com)

## Sending Suspicious Files to Trend Micro

If you think you have an infected file but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send in the suspicious file.

You can also send Trend Micro the URL of any website you suspect of being a phish site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and viruses).

- Contact Support using the following URL:

<http://esupport.trendmicro.com/en-us/business/pages/about-support.aspx#contact-support>

## Security Information Center

Comprehensive security information is available at the Trend Micro website:

- List of viruses and malicious mobile code currently "in the wild," or active
- Virus hoaxes
- Internet threat advisories
- Virus weekly report
- Threat Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code

<http://about-threats.trendmicro.com/threatencyclopedia.aspx>

- Glossary of terms

## TrendLabs

TrendLabs<sup>SM</sup> is the global antivirus research and support center of Trend Micro. Located on three continents, TrendLabs has a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" client viruses and malicious codes
- Emergency virus outbreak support
- Email access to antivirus engineers
- Knowledge Base, the Trend Micro online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

## 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>



# Index

## C

- Case Diagnostic Tool, A-3
- contacting, A-2–A-5
  - documentation feedback, A-5
  - Knowledge Base, A-2
  - sending suspicious files, A-4
  - technical support, A-2
  - Trend Micro, A-2–A-5

## D

- documentation, vi
- documentation feedback, A-5

## K

- Knowledge Base, A-2

## O

- OfficeScan server
  - functions, 2-5

## P

- port
  - server listening port, 3-10

## S

- Security Information Center, A-4
- suspicious files, A-4

## T

- technical support, A-2
- TrendLabs, A-5
- Trend Micro
  - contact information, A-3
  - Knowledge Base, A-2
  - Security Information Center, A-4
  - TrendLabs, A-5

## W

- web console, 1-7
  - about, 1-7
- WFBS
  - documentation, vi



**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](http://www.trendmicro.com)

Item Code: WFEM96625/140825