Worry-Free™ Business Security Standard and Advanced Editions

#1 at stopping threats before they reach your business

Installation Guide

Document Part Number: WBEM74599/100819

Release Date: October 2010

Product Name and Version No.: Trend Micro™ Worry-Free™ Business Security 7.0

Document Version No.: 1.02

Protected by U.S. Patent Nos. 5,951,698 and 7,188,369

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

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

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

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

Contents

Chapter 1: Introducing Trend Micro™ Worry-Free™Business Security Standard and Advanced

Chapter 2: Preparing for Installation

Chapter 3: Installing the Server

Chapter 4: Upgrading and Migrating

Chapter 5: Getting Started

Chapter 6: Managing Basic Security Settings

Appendix A: Troubleshooting and Frequently Asked Questions

Appendix B: Getting Help

Appendix C: Glossary

Index

Chapter 1

Introducing Trend Micro™ Worry-Free™ Business Security Standard and Advanced

This chapter provides an overview of Trend Micro Worry-Free Business Security (WFBS).

The topics discussed in this chapter include:

Overview of Trend Micro Worry-Free Business Security

Trend Micro Worry-Free Business Security (WFBS) protects small business users and assets from data theft, identity theft, risky websites, and spam (Advanced only).

Note: This document provides information for both Worry-Free Business Security Standard and Worry-Free Business Security Advanced. Sections and chapters relevant to the Advanced version only are marked as: "(Advanced only)".

Powered by the Trend Micro™ Smart Protection Network, Worry-Free Business Security is:

- **Safer:** Stops viruses, spyware, spam (Advanced only), and Web threats from reaching computers or servers. URL filtering blocks access to risky websites and helps improve user productivity.
- **Smarter:** Fast scans and continuous updates prevent new threats, with minimal impact to users' PCs.
- **Simpler:** Easy to deploy and requiring zero administration, WFBS detects threats more effectively so that you can focus on business instead of security.

What's New

Version 7.0

Version 7.0 of Worry-Free Business Security provides the following new features and enhancements:

- **Mac Client Protection (Advanced only)**
- **Data Loss Prevention via email (Advanced only)**: data loss prevention content filtering policies prevent sensitive information from being distributed outside the network
- **Enhanced ScanMail for Exchange Support (Advanced only)**: supports Microsoft Exchange Server 2010
- **Device Control:** regulates access to USB devices and network resources

- **Customized Installation:** install only needed components
- **Enhanced URL Filtering:** includes Flexible business hour settings and a separate block list from Web Reputation
- **Web Reputation Filter:** scans URLs in email messages and takes a configurable action when detecting malicious URLs. This feature is separate from spam filtering.
- **Email Reputation Services Filter:** helps block spam and malicious emails by checking the IP addresses of incoming emails against one of the world's largest email reputation databases as well as a dynamic reputation database. It helps to identify new spam and phishing sources and stop even zombies and botnets as they first emerge.
- **Simpler and easier Security Agent user interface**
- **Easier replication amongst WFBS servers**
- **Enhanced blocked page with clear explanation and "Continue Browsing" option**

Key Features

Product features for this version include better integration with the Trend Micro Smart Protection Network.

The Trend Micro Smart Protection Network

The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to protect customers from Web threats. The following are key elements of the Smart Protection Network.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products as well as the company's 24/7 threat research centers and technologies. Each new threat identified via a single customer's routine reputation check automatically updates all of the Trend Micro threat databases, blocking any subsequent customer

encounters of a given threat. By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in protection of others. Because the threat information gathered is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected.

Web Reputation

With one of the largest domain-reputation databases in the world, the Trend Micro Web Reputation technology tracks the credibility of Web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. It will then continue to scan sites and block users from accessing infected ones. To increase accuracy and reduce false positives, Trend Micro Web reputation technology assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites since, often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

Email Reputation (Advanced only)

Trend Micro email reputation technology validates IP addresses by checking them against a reputation database of known spam sources and by using a dynamic service that can assess email sender reputation in real time. Reputation ratings are refined through continuous analysis of the IP addresses' "behavior," scope of activity and prior history. Malicious emails are blocked in the cloud based on the sender's IP address, preventing threats such as zombies or botnets from reaching the network or the user's PC.

File Reputation

Trend Micro file reputation technology checks the reputation of each file against an extensive in-the-cloud database before permitting user access. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the

checking process. The cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall client footprint.

Smart Scan

Trend Micro Worry-Free Business Security uses a new technology called Smart Scan. In the past, WFBS clients used Conventional Scan, which involved each client downloading scan-related components to perform scans. With Smart Scan, the client uses the pattern file on the Smart Scan server instead. Only the Scan Server's resources are used for scanning files.

URL Filtering

URL filtering helps you control access to websites to reduce unproductive employee time, decrease Internet bandwidth usage, and create a safer Internet environment. You can choose a level of URL filtering protection or customize which types of websites you want to screen.

Benefits of Protection

The following table describes how the different components of WFBS protect your computers from threats.

TABLE 1-1. Benefits of Protection

THREAT	PROTECTION
Virus/Malware. Virus, Trojans, Worms, Backdoors, and Rootkits **Spyware/Grayware.** Spyware, Dialers, Hacking tools, Password cracking applications, Adware, Joke programs, and Keyloggers	Antivirus and Anti-spyware Scan Engines along with Pattern Files in the Security Agent and Messaging Security Agent

TABLE 1-1. Benefits of Protection (Continued)

THREAT	PROTECTION
Virus/Malware and Spyware/Grayware transmitted through email messages and spam	POP3 Mail Scan in the Security Agent and IMAP Mail Scan in the Messaging Security Agent Protection for Messaging Security Agent for Microsoft™ Exchange Servers
Network Worms/Viruses	Firewall in the Security Agent
Intrusions	Firewall in the Security Agent
Conceivably harmful websites/Phishing sites	Web Reputation and the Trend Micro in a Security Agent
Malicious behavior	Behavior Monitoring in the Security Agent
Fake access points	The Wi-Fi Advisor in the Security Agent
Explicit/restricted content in IM applications	IM Content Filtering in the Security Agent

Defense Components

Antivirus/Anti-spyware

- **Virus Scan Engine (32-bit/64-bit) for the Security Agent and** Messaging Security Agent**:** The scan engine uses the virus pattern file to detect virus/malware and other security risks on files that your users are opening and/or saving.

  The scan engine works together with the virus pattern file to perform the first level of detection using a process called pattern matching. Since each virus contains a unique "signature" or string of tell-tale characters that distinguish it from any other code, Trend Micro captures inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to patterns in the virus pattern file, searching for a match.

- **Virus pattern:** A file that helps Security Agents identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.
- **Damage Cleanup Template:** Used by the Damage Cleanup Engine, this template helps identify Trojan files and Trojan processes, worms, and spyware/grayware so the engine can eliminate them.
- **Damage Cleanup Engine (32-bit/64-bit):** The engine that Cleanup Services uses to scan for and remove Trojan files and Trojan processes, worms, and spyware/grayware.
- **IntelliTrap exception pattern:** The exception pattern used by IntelliTrap and the scan engines to scan for malicious code in compressed files.
- **IntelliTrap pattern:** The pattern used by IntelliTrap and the scan engines to scan for malicious code in compressed files.
- **Smart Scan Agent Pattern:** The pattern file that the client uses to identify threats. This pattern file is stored on the Agent machine.
- **Smart Feedback Engine (32-bit** and **64-bit)**: The engine for sending feedback to the Trend Micro Smart Protection Network.
- **Smart Scan Pattern:** The pattern file containing data specific to the files on your client's computers.
- **Spyware scan engine (32-bit/64-bit):** A separate scan engine that scans for, detects, and removes spyware/grayware from infected computers and servers running on i386 (32-bit) and x64 (64-bit) operating systems.
- **Spyware/Grayware Pattern v.6:** Contains known spyware signatures and is used by the spyware scan engines (both 32-bit and 64-bit) to detect spyware/grayware on computers and servers for Manual and Scheduled Scans.
- **Spyware/Grayware Pattern:** Similar to the Spyware/Grayware Pattern v.6, but is used by the scan engine for anti-spyware scanning.

Anti-spam

- **Anti-spam engine (32-bit/64-bit):** Detects unsolicited commercial email messages (UCEs) or unsolicited bulk email messages (UBEs), otherwise known as spam.
- **Anti-spam pattern:** Contains spam definitions to enable the anti-spam engine to detect spam in email messages.

- **Email Reputation Services (ERS):** Stops a large amount of spam before it hits the gateway and floods the messaging infrastructure.

Outbreak Defense

Outbreak Defense provides early warning of Internet threats and/or other world-wide outbreak conditions. Outbreak Defense automatically responds with preventative measures to keep your computers and network safe, followed by protection measures to identify the problem and repair the damage.

- **Vulnerability Assessment Pattern:** A file that includes the database for all vulnerabilities. The Vulnerability Assessment Pattern provides instructions for the scan engine to scan for known vulnerabilities.

Network Virus

- **Firewall Driver (Windows XP, 32-bit/64-bit):** The Firewall uses this engine, together with the network virus pattern file, to protect computers from hacker attacks and network viruses.
- **Firewall Pattern:** Like the virus pattern file, this file helps WFBS identify network virus signatures.
- **Transport Driver Interface (TDI) (32-bit/64-bit):** The module that redirects network traffic to the scan modules.
- **Firewall Driver (Windows Vista/7, 32-bit/64-bit):** For Windows™ Vista clients, the Firewall uses this driver with the network virus pattern file to scan for network viruses.

Web Reputation

- **Trend Micro Security database:** Web Reputation evaluates the potential security risk of the requested Web page before displaying it. Depending on the rating returned by the database and the security level configured, the Security Agent will either block or approve the request.
- **URL Filtering Engine (32-bit/64-bit):** The engine that queries the Trend Micro Security database to evaluate the page.

Trend Micro Toolbar

- **Trend Micro Security database:** The Trend Micro Toolbar evaluates the potential security risk of the hyperlinks displayed on a Web page. Depending on the rating returned by the database and the security level configured on the browser plug-in, the plug-in will rate the link.

Software Protection

- **Software Protection List:** Protected program files (`EXE` and `DLL`) cannot be modified or deleted. To uninstall, update, or upgrade a program, temporarily remove the protection from the folder.

Behavior Monitoring

- **Behavior Monitoring Core Driver:** This driver detects process behavior on clients.
- **Behavior Monitoring Core Library :** SA uses this service to handle the Behavior Monitor Core Drivers.
- **Policy Enforcement Pattern:** The list of policies configured on the Security Server that must be enforced by Agents.
- **Digital Signature Pattern:** List of Trend Micro-accepted companies whose software is safe to use.
- **Behavior Monitoring Configuration Pattern:** This pattern stores the default Behavior Monitoring Policies. Files in this pattern will be skipped by all policy matches.
- **Behavior Monitoring Detection Pattern:** A pattern containing the rules for detecting suspicious threat behavior.

Wi-Fi Advisor

- **Wi-Fi Advisor:** Checks the safety of wireless networks based on the validity of their SSIDs, authentication methods, and encryption requirements.

Content Filtering

- **Restricted Words/Phrases List:** The Restricted Words/Phrases List comprises words/phrases that cannot be transmitted through instant messaging applications.

Live Status and Notifications

- The Live Status screen gives you an at-a-glance security status for Outbreak Defense, Antivirus, Anti-spyware, and Network Viruses. If WFBS is protecting Microsoft Exchange servers (Advanced only), you can also view Anti-spam status. Similarly, WFBS can send Administrators notifications whenever significant events occur.

Understanding Threats

The following is a discussion of these terms and their meanings as used in this document.

Virus/Malware

A computer virus/malware is a program – a piece of executable code – that has the unique ability to replicate. Virus/malware can attach themselves to just about any type of executable file and are spread as files that are copied and sent from individual to individual.

In addition to replication, some computer virus/malware share another commonality: a routine that delivers the virus payload. While some payloads can only display messages or images, some can also destroy files, reformat your hard drive, or cause other damage.

- **Malware:** A malware is a program that performs unexpected or unauthorized actions. It is a general term used to refer to viruses, Trojans, and worms. Malware, depending on their type, may or may not include replicating and non-replicating malicious code.
- **Trojans:** Trojans are not viruses. They do not infect files, and they do not replicate. They are malicious programs that masquerades as harmless applications.

  An application that claims to rid your computer of virus/malware when it actually introduces virus/malware into your computer is an example of a Trojan. It may open a port in the background and let malicious hackers take control of the computer. One common scheme is to hijack the computer to distribute spam.

  Because a Trojan does not infect a file, there is nothing to clean, though the scan engine may report the file as "uncleanable" and delete or quarantine it.

With Trojans, however, simply deleting or quarantining is often not enough. You must also clean up after it; that is, remove any programs that may have been copied to the machine, close ports, and remove registry entries.

- **Worms:** A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments. Unlike virus/malware, worms do not need to attach themselves to host programs.
- **Backdoors:** A backdoor is a method of bypassing normal authentication, securing remote access to a computer, and/or obtaining access to information, while attempting to remain undetected.
- **Rootkit:** A rootkit is a set of programs designed to corrupt the legitimate control of an operating system by its users. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security.
- **Macro Viruses:** Macro viruses are application-specific. The viruses reside within files for applications such as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications such as .doc, .xls, and .ppt. Macro viruses travel amongst data files in the application and can eventually infect hundreds of files if undeterred.
- **Mixed Threat Attack:** Mixed threat attacks take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the "Nimda" or "Code Red" threats.

The Agent programs on the client computers, referred to as the Security Agents and Messaging Security Agents, can detect virus/malware during Antivirus scanning. The Trend Micro recommended action for virus/malware is *clean*.

Spyware/Grayware

Grayware is a program that performs unexpected or unauthorized actions. It is a general term used to refer to spyware, adware, dialers, joke programs, remote access tools, and any other unwelcome files and programs. Depending on its type, it may or may not include replicating and non-replicating malicious code.

- **Spyware:** Spyware is computer software that is installed on a computer without the user's consent or knowledge and collects and transmits personal information.

- **Dialers:** Dialers are necessary to connect to the Internet for non-broadband connections. Malicious dialers are designed to connect through premium-rate numbers instead of directly connecting to your ISP. Providers of these malicious dialers pocket the additional money. Other uses of dialers include transmitting personal information and downloading malicious software.
- **Hacking Tools:** A hacking tool is a program, or a set of programs, designed to assist hacking.
- **Adware:** Adware, or advertising-supported software, is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- **Keyloggers:** A keylogger is computer software that logs all the keystrokes of the user. This information could then be retrieved by a hacker and used for his/her personal use.
- **Bots:** A bot (short for "robot") is a program that operates as an agent for a user or another program or simulates a human activity. Bots, once executed, can replicate, compress, and distribute copies of themselves. Bots can be used to coordinate an automated attack on networked computers.

Security Agents and Messaging Security Agents can detect grayware. The Trend Micro recommended action for spyware/grayware is *clean*.

Network Viruses

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the threats mentioned in this section, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate.

Firewall works with a network virus pattern file to identify and block network viruses.

Spam

Spam consists of unsolicited email messages (junk email messages), often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups. There are two kinds of spam: Unsolicited commercial email messages (UCEs) or unsolicited bulk email messages (UBEs).

Intrusions

Intrusions refer to entry into a network or a computer either by force or without permission. It could also mean bypassing the security of a network or computer.

Malicious Behavior

Malicious Behavior refers to unauthorized changes by software to the operating system, registry entries, other software, or files and folders.

Fake Access Points

Fake Access Points, also known as Evil Twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications.

Explicit/Restricted Content in IM Applications

Text content that is either explicit or restricted to your organization being transmitted over instant messaging applications. For example, confidential company information.

Online Keystroke Listeners

An online version of a keylogger. See *Spyware/Grayware* on page 1-11 for more information.

Packers

Packers are tools to compress executable programs. Compressing an executable makes the code contained in the executable more difficult for traditional Antivirus scanning products to detect. A Packer can conceal a Trojan or worm.

The Trend Micro scan engine can detect packed files and the recommended action for packed files is *quarantine*.

Phishing Incidents (Advanced only)

A Phishing incident starts with an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click a link that will redirect their browsers to a fraudulent website. Here the user is asked to update

personal information such as passwords, social security numbers, and credit card numbers in an attempt to trick a recipient into providing private information that may be used for identity theft.

Messaging Security Agents use Anti-spam to detect phishing incidents. The Trend Micro recommended action for phishing incidents is *delete entire message* in which it detected the phish.

Mass-Mailing Attacks (Advanced only)

Email-aware virus/malware have the ability to spread by email message by automating the infected computer's email clients or by spreading the virus/malware themselves. Mass-mailing behavior describes a situation when an infection spreads rapidly in a Microsoft Exchange environment. Trend Micro designed the scan engine to detect behavior that mass-mailing attacks usually demonstrate. The behaviors are recorded in the Virus Pattern file that is updated using the Trend Micro ActiveUpdate Servers.

You can enable the MSA to take a special action against mass-mailing attacks whenever it detects a mass-mailing behavior. The action set for mass-mailing behavior takes precedence over all other actions. The default action against mass-mailing attacks is delete entire message.

For example: You configure the MSA to quarantine messages when it detects that the messages are infected by a worm or a Trojan. You also enable mass-mailing behavior and set the MSA to delete all messages that demonstrate mass-mailing behavior. the MSA receives a message containing a worm such as a variant of MyDoom. This worm uses its own SMTP engine to send itself to email addresses that it collects from the infected computer. When the MSA detects the MyDoom worm and recognizes its mass-mailing behavior, it will delete the email message containing the worm - as opposed to the quarantine action for worms that do not show mass-mailing behavior.

Network Components

Worry-Free Business Security uses the following components:

TABLE 1-2. Network Components

CONVENTION/TERM	DESCRIPTION
Security Server	The Security Server hosts the Web Console, the centralized Web-based management console for the entire Trend Micro™ Worry-Free™ Business Security solution.
Web Console	The Web Console is a centralized, management console that manages all the Agents. The Web Console resides on the Security Server.
Agent/SA/MSA	The Security Agent or Messaging Security Agent (Advanced only). Agents protect the Client it is installed on.
Clients	Clients are Microsoft Exchange servers, desktops, portable computers, and servers where a Messaging Security Agent or a Security Agent is installed.
Scan Server	A Scan Server helps scan clients that are configured for Smart Scan. By default, a Scan Server is installed on the Security Server.

Sending Trend Micro Your Viruses

If you have a file you think is infected but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us. For more information, see the following site:

http://subwiz.trendmicro.com/subwiz

Please include in the message text a brief description of the symptoms you are experiencing. The team of antivirus engineers will analyze the file to identify and characterize any viruses it may contain, usually the same day it is received.

Chapter 2

Preparing for Installation

The steps in this phase help you develop a plan for Worry-Free Business Security installation and deployment. Trend Micro recommends creating an installation and deployment plan before the installation. This will help ensure that you incorporate the product's capabilities into your existing antivirus and network protection initiative.

The topics discussed in this chapter include:

Before You Begin

Review the following phases of installation and deployment.

Phase 1: Deployment Planning

Planning the WFBS deployment includes the following tasks:

1. Verifying system requirements. Refer to *Server and Agent System Requirements* on page 2-4 for more information.
2. Determining where to install the Security Server. Refer to *Determining Where to Install the Security Server* on page 2-28 for more information.
3. Identifying the number of clients. Refer to *Identifying the Number of Clients* on page 2-29 for more information.
4. Planning for network traffic. Refer to *Planning for Network Traffic* on page 2-29 for more information.
5. Determining desktop and server groups. Refer to *Determining the Number of Desktop and Server Groups* on page 2-31 for more information.
6. Choosing installation/deployment options for Security Agents. Refer to *Choosing Deployment Options for Security Agents* on page 2-32 for more information.

Phase 2: Installing the Security Server

This phase includes the following tasks:

1. Preparing the target server for installation. Refer to *Server and Agent System Requirements* on page 2-4 for more information.

   Tip: Refer to the System Checklists section of the WFBS *Administrator's Guide* for details.

2. Installing or upgrading WFBS. Refer to *Installation Overview* on page 2-23 or *Upgrading Best Practices* on page 4-3 for more information.
3. Verifying the installation. Refer to *Verifying the Installation* on page 3-35 for more information.

Phase 3: Installing Agents

After installing the Security Server, install Security Agents on all the servers and desktops and install Messaging Security Agents on the Exchange servers. This phase includes the following tasks:

Note: Refer to the *Administrator's Guide* for an overview.

1. Selecting an installation method
2. Installing or upgrading agents
3. Verifying the installation
4. Testing the installation

Phase 4: Configuring Security Options

After installing Security Agents on the clients, customize the default settings if required. This includes the following tasks:

1. Configuring server and desktop groups
2. Configuring Microsoft Exchange servers
3. Configuring preferences

Server and Agent System Requirements

To install WFBS Security Server (which includes the Scan Server) and the Security Agents, the following specifications are required:

TABLE 2-1. System Requirements

ITEM	MINIMUM SPECIFICATIONS	
Security Server		
Processor	• Conventional scan mode: Intel™ Pentium™ 4 or higher • Smart Scan mode: Multiple processors or multi-core processor	
Memory	• Smart Scan mode: 1GB; 2GB recommended • Conventional mode(x86) : 512MB ; 1GB recommended • X64 (Smart and Conventional) : 1GB ; 2GB recommended • Windows EBS 2008 or Windows SBS 2008 (Smart and Conventional): 4GB	
Disk space	6GB total disk space (excludes SA and MSA disk usage) • 3GB for installation • 3GB for operation	

TABLE 2-1. System Requirements (Continued)

ITEM	MINIMUM SPECIFICATIONS	
Operating System	**Series or Family**	**Supported Service Packs or Releases**
	Windows XP	Professional Edition with SP3 Media Center 2005 Edition with SP3
	Windows Vista	Ultimate with SP1 or SP2 Enterprise with SP1 or SP2 Business with SP1 or SP2 Home Premium with SP1 or SP2 Home Basic with SP1 or SP2
	Windows 7	Ultimate, no service pack or SP1 Enterprise, no service pack or SP1 Professional, no service pack or SP1 Home Premium, no service pack or SP1 Home Basic, no service pack or SP1 **Note:** Windows 7 Starter edition is not supported
	Windows Server 2003	Web Edition with SP1 or SP2 Standard Edition with SP1 or SP2 Enterprise Edition with SP1 or SP2 Datacenter Edition with SP1 or SP2
	Windows Small Business Server (SBS) 2003	SP1 or SP2
	Windows Storage Server 2003	No service pack

TABLE 2-1. System Requirements (Continued)

ITEM	MINIMUM SPECIFICATIONS	
	Windows SBS 2003 R2	Web Edition with SP1 or SP2 Standard Edition with SP1 or SP2 Enterprise Edition with SP1 or SP2 Datacenter Edition with SP1 or SP2
	Windows Home Server	No service pack or Power Pack 1 or 3
	Windows Server 2008	Standard Edition, no service pack or SP2 Enterprise Edition, no service pack or SP2 Datacenter Edition, no service pack or SP2
	Windows SBS 2008	Standard Edition, no service pack or SP2 Premium Edition, no service pack or SP2
	Windows Essential Business Server (EBS) 2008	Standard Edition, no service pack or SP2 Premium Edition, no service pack or SP2
	Windows Storage Server 2008	No service pack

TABLE 2-1. System Requirements (Continued)

ITEM	MINIMUM SPECIFICATIONS	
	Windows Server 2008 R2	Foundation Edition, no service pack or SP1(RC) Standard Edition, no service pack or SP1(RC) Enterprise Edition, no service pack or SP1(RC) Datacenter Edition, no service pack or SP1(RC)
	Windows Small Business Server 7 Beta	No Service Pack
	Windows Home Server V2 Beta	No Service Pack
	Notes: • Windows Server 2008 and 2008 R2 installations that use the Server Core option are not supported. • All major editions and 64-bit versions of the listed operating systems are supported unless noted otherwise. • Basic coverage in Windows SBS 7 and Windows Home Server V2, full support to be released in WFBS7 Service Pack.	

TABLE 2-1. System Requirements (Continued)

ITEM	MINIMUM SPECIFICATIONS
Web server	• IIS 6.0 (Windows Server 2003, SBS 2003, or Home Server) • IIS 7.0 (Windows Server 2008, SBS 2008, or EBS 2008) • IIS 7.5 (Windows Server 2008 R2) • Apache™ HTTP Server 2.0.63 or later **Note:** IIS is not supported on Windows XP or Windows Vista/7. Apache must be used on these operating systems. If you already have an Apache server installed, Trend Micro recommends uninstalling it. An appropriate Apache server will be installed together with the Security Server.
Management Console	
Web browser	Internet Explorer 6.0 SP2 or later (32-bit only)
PDF reader (for reports)	Adobe™ Acrobat™ Reader 6.0 or later
Display	High-color display with a resolution of 1024x768 or higher
Security Agent	

Processor	• Intel™ Pentium™ x86 or compatible processor
	• x64 processor supporting AMD64 and Intel EM64T technologies
	• Clock speed requirements vary depending on the operating system:
	  • 1GHz (Windows Server 2008, SBS 2008, or EBS 2008)
	  • 800MHz (Windows Vista, Windows 7)
	  • 450MHz (Windows XP, Server 2003, SBS 2003, or Home Server)

TABLE 2-1. System Requirements (Continued)

ITEM	MINIMUM SPECIFICATIONS
Memory	• 4GB (SBS/EBS 2008) • 1GB minimum; 2GB recommended (Windows Server 2008 or SBS 2003) • 512MB minimum; 1GB recommended (Windows Vista, Windows 7) • 512MB minimum; 1GB recommended (Windows Server 2003, or Home Server) • 256MB minimum; 512MB recommended (Windows XP)
Disk space	Smart Scan 500MB total disk space • 300MB for installation • 200MB for operation Conventional Scan 1GB total disk space • 400MB for installation • 600MB for operation
Operating System	**The Security Agent supports all operating systems supported by the Security Server.** In addition to these operating systems, the SA also supports: • Windows XP Home (SP3) • Windows XP Tablet (SP3)
Web browser (for Web-based setup)	Internet Explorer 6.0 SP2 or later
Display	256-color display or higher with resolutions of 800x600 or higher

TABLE 2-1. System Requirements (Continued)

ITEM	MINIMUM SPECIFICATIONS	
Messaging Security Agent		
Processor	• 1GHz Intel Pentium x86 or compatible processor • 1GHz processor supporting AMD64 and Intel EM64T technologies	
Memory	1GB	
Disk space	2GB total disk space • 500MB for installation • 1.5GB for operation	
Operating system	**Series or Family**	**Supported Service Packs or Releases**
	Windows Server 2003 R2 (with Storage Server 2003)	SP1 or SP2
	Windows Server 2003 (with Storage Server 2003)	SP1 or SP2
	Windows SBS 2003 R2	SP1 or SP2
	Windows SBS 2003	SP1 or SP2
	Windows Server 2008	SP1 or SP2
	Windows Server 2008 R2	No service pack
	Windows SBS 2008	SP1 or SP2
	Windows EBS 2008	SP1 or SP2

TABLE 2-1. System Requirements (Continued)

ITEM	MINIMUM SPECIFICATIONS
	Note: All major editions and 64-bit versions of these operating systems are supported unless noted otherwise.
Web server	• IIS 6.0 (Windows Server 2003, SBS 2003, or Home Server) • IIS 7.0 (Window Server 2008, SBS 2008, or EBS 2008) • IIS 7.5 (Windows Server 2008 R2)
Mail server	Exchange Server 2003 SP2 or above. Exchange 2007 SP1 or above, and Exchange 2010 **Note:** To integrate properly with the anti-spam features in Exchange Server 2003 and 2007, the Messaging Security Agent requires the Intelligent Message Filter on these versions of Exchange Server.

Notes

- Security Agents support Citrix Presentation Server™ 4.0/4.5/5.0 and Remote Desktop
- Security Agents support Gigabit network interface cards (NICs)
- WFBS 7.0 supports VMware® ESX™ 3.0/3.5, VMware Server 1.0.3/2.0.1, VMware Workstation 6.0/6.5, and Microsoft Hyper-V™ Server 2008

Other Requirements

- Clients that use Smart Scan must be in online mode. Offline clients cannot use Smart Scan
- Administrator or Domain Administrator access on the computer hosting the Security Server
- File and printer sharing for Microsoft Networks installed
- Transmission Control Protocol/Internet Protocol (TCP/IP) support installed

- If Microsoft ISA Server or a proxy product is installed on the network, you need to open the HTTP port (8059 by default) and the SSL port (4343 by default) to allow access to the Web Console and to enable client-server communications

Choosing Your Edition

Installing Worry-Free Business Security

Worry-Free Business Security and Worry-Free Business Security Advanced use the same installation program. The version that you install depends on the Activation Code that you provide during the installation process.

Trend Micro offers the following versions:

- **Worry-Free Business Security:** Designed to protect desktops, portable computers, and servers on your local network. Includes Outbreak Defense, Firewall, and Antivirus and Anti-spyware scanning. The standard version of WFBS 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 the Microsoft Exchange servers on your network. Includes all the features of Worry-Free Business Security plus Anti-spam, Content Filtering, and Attachment Blocking.

If you have an Activation Code for Worry-Free Business Security Advanced, the installation program provides you with an option of installing the Messaging Security Agent on your Microsoft Exchange servers.

During installation, Setup prompts you to enter an Activation Code. If you leave the field empty, Worry-Free Business Security installs the evaluation version.

Note: The 30-day evaluation version is installed by default when you do not provide an Activation Code. You can also install an evaluation version without a Registration Key or Activation Code. To find out more information, contact your Trend Micro sales representative (see *Contacting Trend Micro* on page B-4).

Registering Worry-Free Business Security

You need to register and activate this application to enable pattern file and scan engine updates. When you purchase WFBS 7.0, you will receive a Registration Key.

A Registration Key is 22 characters in length, including hyphens, in the following format:

xx-xxxx-xxxxx-xxxxx-xxxxx

You can use this Registration Key to register on the Trend Micro website at http://olr.trendmicro.com.

Note: If you purchase the Trend Micro SMB Solution CD, you can find an evaluation Registration Key on the packing. Use this key to register online and obtain your personal Activation Code via email.

Activation Code

After registering, you will receive a personal Activation Code via email. An Activation Code has 37 characters (including the hyphens) and looks like this:

xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

You automatically receive an evaluation Activation Code if you download Worry-Free Business Security 7.0 from the Trend Micro website.

During the installation program, you need to provide your activation code to validate WFBS 7.0.

Note: When the evaluation period ends, the Security Server no longer receives updated components unless you key in your personal Activation Code in the Web Console.

License and Maintenance Agreement

When you purchase Worry-Free Business Security or Worry-Free Business Security Advanced, 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.

Sixty (60) days before your Maintenance Agreement expires, the Live Status screen on the Web Console will display a message, warning you to renew your license. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales person, or on the Trend Micro website at:

https://olr.trendmicro.com/registration/

Consequences of an Expired License

When a fully licensed version 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 WFBS by purchasing a maintenance renewal. You need an Activation Code to install the full versions.

Note: 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

Worry-Free Business Security and Worry-Free Business Security Advanced

The following table lists the features supported for each edition.

TABLE 2-2. Features Available by Product Editions

FEATURES	WORRY-FREE BUSINESS SECURITY	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
Instant Messaging Content Filtering	Yes	Yes
Mail Scan (POP3)	Yes	Yes
Anti-Spam (POP3)	Yes	Yes
Mail Scan (IMAP)	No	Yes
Anti-Spam (IMAP)	No	Yes
Email Message Content Filtering	No	Yes
Email Message Data Loss Prevention	No	Yes
Attachment Blocking	No	Yes

The following table lists the features supported for each type of license.

TABLE 2-3. License Status Consequences

	Fully Licensed	Evaluation (30 days)	Expired
Expiration Notification	Yes	Yes	Yes
Malware/Virus Pattern File Updates	Yes	Yes	No
Program Updates	Yes	Yes	No
Technical Support	Yes	No	No
Real-time Scanning*	Yes	Yes	No

*For expired licenses, real-time scan will use outdated components.

Note: To upgrade your edition, contact a Trend Micro sales representative.

Protecting Your Network

WFBS protection consists of the following components:

- **Management Console:** Manages all agents from a single location
- **Security Server:** Hosts the Web Console, downloads updates from the Trend Micro ActiveUpdate Server, collects and stores logs, and helps control virus/malware outbreaks
- **Security Agent**: Protects Windows 7/Vista/XP/Server 2003/Server 2008 computers from malware/viruses, spyware/grayware, Trojans, and other threats
- **Messaging Security Agent:** Protects Microsoft Exchange servers, filters spam, and blocks malicious content

- **Scan Server:** Downloads scanning-specific components from Trend Micro and uses them to scan clients

Note: In the WFBS implementation of the Smart Scan, the same computer acts as both the Security Server and the Smart Scan server.

The following figure illustrates how the WFBS components are installed on a typical network.

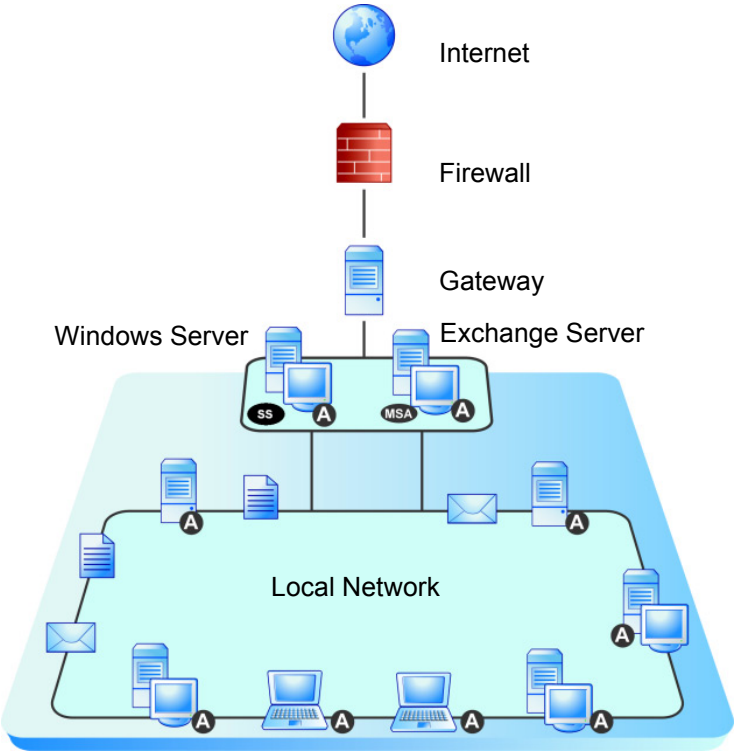


FIGURE 2-1. Network topology example

TABLE 2-4. Network Topology Example Descriptions

SYMBOL	DESCRIPTION
A	Security Agent installed on clients
MSA	Messaging Security Agent installed on an Exchange server (only available in Worry-Free Business Security Advanced)
SS	Security Server and Scan Server installed on a Windows server

The Web Console

The Web Console is a centralized Web-based management console for WFBS. Use the Web Console to configure Security Agents. The Web Console is installed when you install the Trend Micro Security Server and uses Internet technologies such as ActiveX, CGI, HTML, and HTTP/HTTPS.

You can use the Web Console to:

- Deploy the Security Agents to servers, desktops, and portable computers
- Combine desktops and portable computers and servers into logical groups for simultaneous configuration and management
- Set antivirus and anti-spyware scan configurations and start a Manual Scan on a single group or on multiple groups
- Receive notifications and view log reports for virus/malware activities
- Receive notifications and send outbreak alerts through email messages, SNMP Trap, or Windows Event Log when threats are detected on clients
- Control outbreaks by configuring and enabling Outbreak Prevention

Security Server

At the center of WFBS is the Security Server (indicated by **SS** in *Figure 2-1*). The Security Server hosts the Web-based management console for WFBS. The Security Server installs Security Agents on clients on the network and creates a client-server relationship. The Security Server enables viewing security status information, viewing Security Agents, configuring system security, and downloading components from a centralized location. The Security Server also contains a database where it stores logs of detected Internet threats being reported to it by the Security Agents.

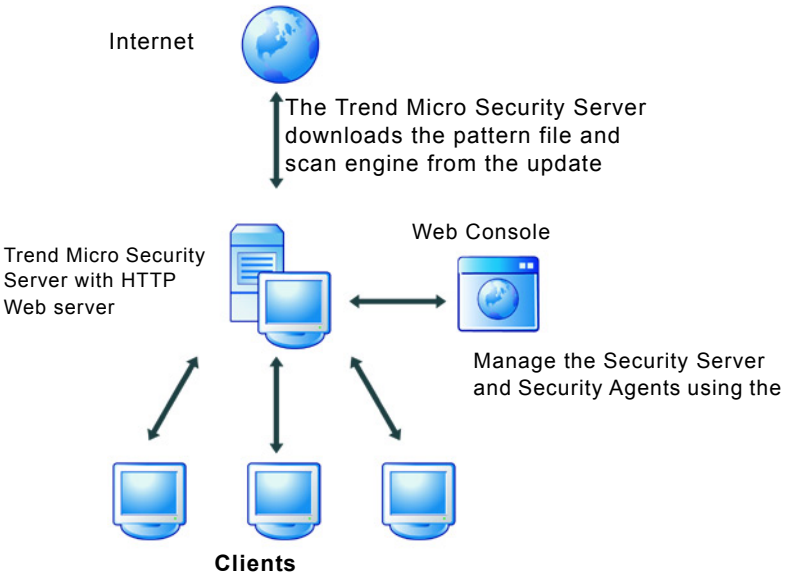


FIGURE 2-2. How Client/Server communication through HTTP works

Security Agent

The Security Agent (indicated by **A** in *Figure 2-1*) reports to the Trend Micro Security Server from which it was installed. To provide the Security Server with the very latest client information, the Security Agent sends event status information in real-time. Security Agents report events such as threat detection, Agent startup, Agent shutdown, start of a scan, and completion of an update.

The Security Agent provides three methods of scanning: Real-time Scan, Scheduled Scan, and Manual Scan.

You can configure scan settings on Security Agents from the Web Console. To enforce uniform desktop protection across the network, choose not to grant user privileges to modify the scan settings or to remove the Security Agent.

Scan Server

As part of the Smart Protection Network, WFBS 7.0 now provides the ability to scan your clients with a Scan Server. This takes the burden of downloading components and scanning clients off your client computers and puts it on a Scan Server.

There are two types of Scan Servers:

- **Scan Server:** A Scan Server is automatically installed with the Security Server. This allows your server to act as a both centralized control center for your Security Agents and as a security scanner.
- **Trend Micro Global Smart Scan Server:** Trend Micro provides a Scan Server for all clients as a backup. If the Scan Server on your network fails for any reason, Trend Micro provides you with the necessary protection.

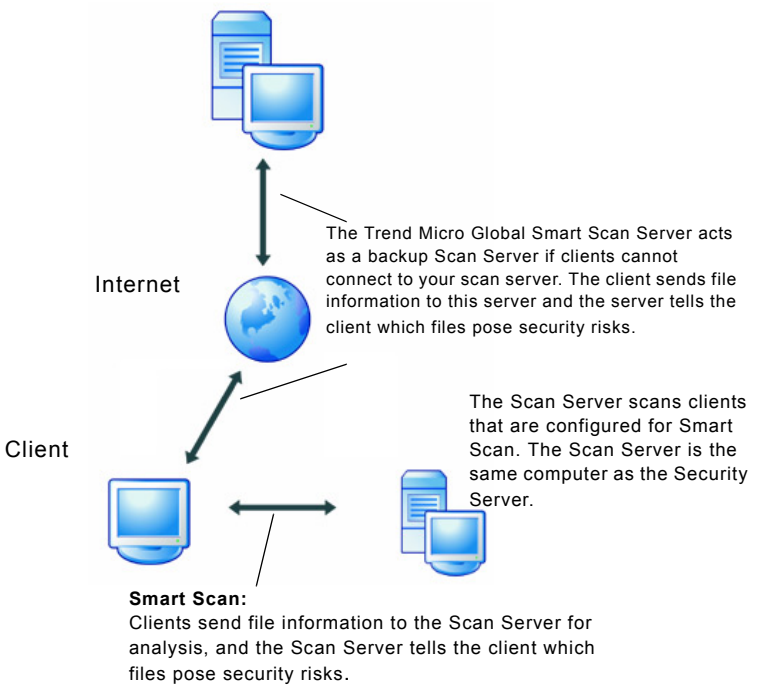


FIGURE 2-3. How Smart Scan communication works

Note: The Scan Server is automatically installed with the Security Server. After installation, you can specify which computers will use the Scan Server.

Installation Overview

The setup program will prompt you for the following information during installation:

- **Security Server details:** The domain/hostname or the IP address of the Security Server and the target folder where WFBS installs the Security Server files
- **Proxy server details:** If a proxy server handles Internet traffic on your network, you must configure proxy server information (if required, the user name and password too). This information is necessary to download the latest components from the Trend Micro update server. You can enter proxy server information during or after installation. Use the Web Console to enter information after installation.
- **SMTP server:** If using an SMTP server to send notifications, enter the name of the SMTP server, the port number, and the sender's and recipients' email addresses.

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

- **Security Server Web Console password:** To prevent unauthorized access to the Web Console, specify a password
- **Client unload/uninstall password:** Set a password to prevent unauthorized unloading or removal of the Security Agent
- **Client software installation path:** Configure the client installation path where the Security Agent files will be copied to during client setup
- **Account and Privileges:** Before proceeding with the installation, log on using an account with either domain or local administrator privileges
- **Restarting services:** You do not need to stop or start Microsoft Exchange services before or after the installation. When uninstalling or upgrading the Trend Micro Messaging Security Agent, the IIS Admin service/Apache server and all related services will automatically be stopped and restarted.

WARNING! 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.

Ports

WFBS uses two types of ports:

- **Server listening port (HTTP port):** Used to access the Trend Micro 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 Client receives commands from the Trend Micro Security Server.
- **Scan Server ports:** Used to scan your agents. See *Table 2-5*:

TABLE 2-5. Scan Server Ports

	IIS DEFAULT	IIS VIRTUAL	PRE-INSTALLED APACHE	NEW APACHE INSTALLATION
FRESH INSTALLS AND UPGRADES				
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

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.

Trend Micro Security Server Prescan

Before the setup program begins the installation process, it performs a prescan. This prescan includes a malware/virus scan and a Damage Cleanup Services scan to help ensure the target computer does not contain malware, Trojans, or other potentially malicious code.

The prescan targets the most vulnerable areas of the computer, which include the following:

- the Boot area and boot directory (for boot sector viruses)
- the Windows folder
- the Program Files folder

Actions for Prescan Detections

If the WFBS setup program detects malware, spyware/grayware, or other potentially malicious code, you can take the following actions:

- **Clean:** Cleans an infected file by removing the malware or malicious application. WFBS encrypts and renames the file if the file cannot be cleaned
- **Delete:** Deletes the file
- **Pass:** Does nothing to the file

Tip: Trend Micro recommends cleaning or deleting infected files.

Other Installation Notes

Installing the Trend Micro Security Server does not require you to restart the computer. After completing the installation, immediately configure the Trend Micro Security Server and then proceed to roll out the Security Agent program. If using an IIS web server, the setup program automatically stops and restarts the IIS/Apache service during the Security Server installation.

WARNING! **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.**

Tip: Trend Micro recommends installing WFBS during non-peak hours to minimize the impact on your network.

If a non-supported version of the Apache Web server is already installed on the Security Server, use IIS instead of Apache. If two Web server applications are running at the same time, verify that the port numbers do not conflict, and that the computer has enough memory, CPU power, and disk resources.

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 components.

Other Antivirus Applications

Trend Micro recommends removing other antivirus applications from the computer on which you will install the Trend Micro Security Server. The existence of other antivirus applications on the same computer may hinder a proper Trend Micro Security Server installation and influence its performance.

Note: WFBS cannot uninstall the server component of any third-party antivirus product but can uninstall the client component (see *Migrating from Other Anti-Malware Applications* on page 4-4 for instructions and for a list of third-party applications WFBS can remove).

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.

MSA and Forefront

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

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 client computers.

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 (including Internet Connection Firewall (ICF) provided by Windows 7, Windows Vista, Windows XP SP3, and Windows Server 2003) if you want to install the WFBS firewall. 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 *Ports* on page 2-24 for information on listening ports and refer to your firewall documentation for details on how to configure exception lists).

Deployment Checklist

Look over the following before you deploy WFBS.

Determining Where to Install the Security Server

WFBS is flexible enough to 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 managing more than one site, having a Security Server at the main site as well as at each managed site will reduce bandwidth usage between the main site and managed sites, and 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.

Identifying the 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.

If your network has different Windows operating systems, such as Windows XP, Windows Server 2003, Windows Vista or Windows 7, identify how many clients are using a specific Windows version. Use this information to decide which client deployment method will work best in your environment. Refer to *Choosing Deployment Options for Security Agents* on page 2-32.

Note: 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.

Planning for Network Traffic

When planning for deployment, consider the network traffic that WFBS will generate. WFBS generates network traffic when the Security Server and clients communicate with each other.

The Security Server/Scan Server generates traffic when:

- Notifying clients about configuration changes
- Notifying clients to download updated components
- Connecting to the Trend Micro ActiveUpdate Server to check for and download updated components
- Performing scans on the clients that are configured for Smart Scan
- Sending feedback to the Trend Micro Smart Protection Network

Clients generate traffic when:

- Starting up
- Shutting down
- Generating logs
- Performing scheduled updates

- Performing manual updates ("Update Now")
- Connecting to the Scan Server for Smart Scan

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

Network Traffic during Pattern File Updates

Significant network traffic is generated whenever Trend Micro releases an updated version of any product component.

To reduce network traffic generated during pattern file updates, WFBS uses a method called incremental update. Instead of downloading the full updated pattern file every time, the Trend Micro Security Server only downloads the new patterns that have been added since the last release. The Trend Micro Security Server merges the new patterns with the old pattern file.

Regularly updated clients only have to download the incremental pattern file, which is approximately 5KB to 200KB. The full pattern file is approximately 50MB when compressed and takes substantially longer to download.

Trend Micro releases new pattern files daily. However, if a particularly damaging malware is actively circulating, Trend Micro releases a new pattern file as soon as a pattern for the threat is available.

Using Update Agents to Reduce Network Bandwidth

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

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 client on each segment to act as an Update Agent.

Deciding on a Dedicated Server

When selecting a server that will host WFBS, consider the following:

- How much CPU load is the server carrying?
- What other functions does the server perform?

If you consider installing WFBS on a server that has other uses (for example, an application server), Trend Micro recommends that you install WFBS on a server that is not running mission-critical or resource-intensive applications.

Location of the Program Files

During the Trend Micro Security Server installation, specify where to install the program files on the clients. Either accept the default client installation path or modify it. Trend Micro recommends that you use the default settings, unless you have a compelling reason (such as insufficient disk space) to change them.

The default client installation path is:

```
C:\Program Files\Trend Micro\Security Agent
```

Determining the Number of Desktop and Server Groups

Every Security Agent must belong to a security group. The members of a security group all share the same configuration and run the same tasks. By organizing clients in groups, you can simultaneously configure, manage, and apply a customized configuration to one group without affecting the configuration of other groups.

Note: You cannot group multiple Exchange servers into a group.

A WFBS security group is different from a Windows domain. You can create multiple security groups within a single Windows domain. You may also assign computers from different Windows domains to the same security group. The only requirement is that all the clients in a group must be registered to the same Security Server.

You can group clients based on the departments they belong to or the functions they perform. Alternatively, you can group clients that are at a greater risk of infection and apply a more secure configuration than you may wish to apply to other clients. You will need at least one group for every unique client configuration that you wish to create.

Choosing Deployment Options for Security Agents

WFBS provides several options to deploy Security Agents. Determine which ones are most suitable for your environment, based on your current management practices and the account privileges that end users have.

For single-site deployment, IT administrators can choose to deploy using **Remote Installation** or **Login Script Setup**. For the Login Script Setup method, a program called `autopcc.exe` is added to the login script. When an unprotected client logs on to the Windows domain, the Security Server detects it and automatically deploys the client setup program. The Security Agent is deployed in the background and the end user does not notice the installation process.

In organizations where IT policies are strictly enforced, Trend Micro recommends to use Remote Install and Login Script Setup. Remote-install and login-script setups do not require to assign administrative privileges to the end user. Instead, the administrator configures the installation program itself with the password to an administrative account. You do not need to modify the end user's permissions.

Note: Remote install works only with Windows 7/Vista/XP (Professional Edition only) and Windows Server 2003/2008

In organizations where IT policies are less strictly enforced, Trend Micro recommends to install Security Agents using the internal Web page. The administrator sends out an email message instructing users to visit an internal Web page where they can install the Security Agent. Using this method, however, requires that end users who will install the Security Agent have administrator privileges.

WFBS includes a tool called the **Vulnerability Scanner**, which can help to detect computers that are not protected by WFBS. Once the Vulnerability Scanner detects an unprotected computer, it deploys the Security Agent to it. When you enter a range of IP

addresses, the Vulnerability Scanner checks every computer within the specified range and reports the current antivirus software version (including third-party software) installed on each computer.

Note: The Vulnerability Scanner only works on 32-bit operating systems.

Note: To install the Security Agent using Vulnerability Scanner, you must have administrator rights. To bypass this problem, you can provide administrator-level login credentials that the Vulnerability Scanner will then use to install the Security Agent.

Client Packager, a WFBS tool, can compress setup and update files into a self-extracting file to simplify delivery through an email message, CD-ROM, or internal FTP. When users receive the package, they have to double-click the file to start the setup program.

Tip: Remote Install is efficient for networks with Active Directory. If your network does not use Active Directory, use Web installation.

For more information about the installation methods, refer to the WFBS *Administrator's Guide*.

Ports Checklist

WFBS uses the following default ports.

TABLE 2-6. Port Checklist

PORT	SAMPLE	YOUR VALUE
SMTP	25	
Proxy	Administrator Defined	
Security Server: Non-SSL Port	8059	
Security Server: SSL Port	4343	

TABLE 2-6. Port Checklist (Continued)

PORT	SAMPLE	YOUR VALUE
Security Agent	21112	
Messaging Security Agent	16372	
Scan Server SSL Port	4345	
Scan Server Non-SSL Port	8082	
Trend Micro Security for Mac Communication Port	61617	

Security Server Address Checklist

WFBS requires the following information during installation and during configuration. Record these details for easy reference.

TABLE 2-7. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
TREND MICRO SECURITY SERVER INFORMATION		
IP address	192.168.1.1	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
WEB SERVER INFORMATION		
IP address	192.168.1.1	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	

TABLE 2-7. Server Address Checklist (Continued)

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
PROXY SERVER FOR COMPONENT DOWNLOAD		
IP address	192.168.1.1	
Fully Qualified Domain Name (FQDN)	proxy.company.com	
NetBIOS (host) name	proxyserver	
SMTP SERVER INFORMATION (OPTIONAL; FOR EMAIL NOTIFICATIONS)		
IP address	192.168.1.1	
Fully Qualified Domain Name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	
SNMP TRAP INFORMATION (OPTIONAL; FOR SNMP TRAP NOTIFICATIONS)		
Community name	company	
IP address	192.168.1.1	

Chapter 3

Installing the Server

This chapter provides information you will need to understand to install Worry-Free Business Security (WFBS).

The topics discussed in this chapter include:

Installation Overview

There are three methods for installing WFBS:

- **Typical (Recommended):** Provides an easy solution for installing WFBS using Trend Micro default values. This method is suitable for a small business using a single Trend Micro Security Server and up to ten clients.
- **Minimal Install**: Provides an entry-level configuration of WFBS that offers robust prevention, threat detection, and remediation using Trend Micro Smart Scan technology that minimizes the impact on system and network resources
- **Custom:** Provides flexibility in implementing your network security strategy. This method is suitable if you have many computers and servers or multiple Exchange servers.
- **Silent:** Performing a Silent installation creates a record file that you can use to perform identical installations on other computers or networks

Tip: You can preserve your client settings when you upgrade to this version of WFBS or if you need to reinstall this version of WFBS. See *Upgrading the Security Agent* on page 4-8.

Note: If information from a previous Messaging Security Agent (MSA) installation exists on the client, you will be unable to install MSA 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

Installing the Scan Server

When you install the Security Server, the Scan Server is automatically installed. You do not need to choose to install the Scan Server or to configure any settings.

Typical Installation Walkthrough

The Typical installation method follows the same flow as the Custom installation method (refer to *Custom Installation Walkthrough* on page 3-3). During a Typical installation, the following options are not available because they use the Trend Micro default settings:

- **WFBS program folder.** `C:\Program Files\Trend Micro\Security Server\PCCSRV`
- **Web server:** Microsoft Internet Information Services (IIS)

Note: If the Security Server (including the Smart Scan service) is installed on Windows XP, Microsoft IIS can support only a maximum of 10 client connections to the Smart Scan service. If clients will use Smart Scan and the Security Server is installed on Windows XP, select the Apache web server instead of IIS.

- **Web server settings**
  - **Website:** OfficeScan
  - **Default URL:** `https://<IP_ADDRESS>:4343/SMB`
- **Security Agent settings:** Refer to the WFBS *Administrator's Guide* for information.

To perform an installation using the Typical Installation method, follow the steps in *Custom Installation Walkthrough* on page 3-3 and ignore the steps that are relevant to Custom Installation.

Custom Installation Walkthrough

The Custom Installation method provides the most flexibility in implementing your network security strategy. The Custom and Typical installation processes follow a similar flow:

1. Perform pre-configuration tasks. Refer to *Part 1: Pre-configuration Tasks* on page 3-4.
2. Enter the settings for the Trend Micro Security Server and the Web Console. Refer to *Part 2: Security Server Settings* on page 3-10.
3. Configure the Security Agent installation options. Refer to *Part 3: Security Agent Installation Options* on page 3-18.

4. Configure the Messaging Security Agent installation options for Microsoft Exchange servers (Advanced only). Refer to *Part 4: Messaging Security Agent Installation Options* on page 3-23
5. Start the installation process. Refer to *Part 5: Installation Process* on page 3-31.

Part 1: Pre-configuration Tasks

The pre-configuration tasks consist of launching the installation wizard, providing licensing and activation details, and choosing an installation type.

Tip: Close any running applications before installing WFBS. If you install while other applications are running, the installation process may take longer to complete.

To start the pre-configuration tasks:

1. Open the folder that contains the setup files and double-click the `SETUP.EXE` file. The **Trend Micro Installation** screen appears.
2. Click **Next**. The **License Agreement** screen appears.
3. Read the license agreement. If you agree with the terms, select **I accept the terms of the license agreement**.

4. Click **Next**. The **Setup Type** screen appears

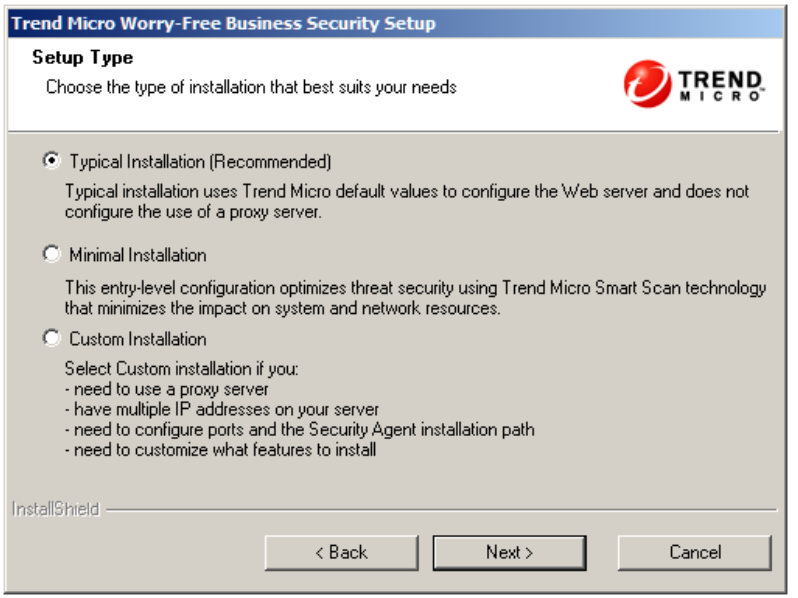


FIGURE 3-1. Setup Type screen

5. From the **Setup Type** screen, choose one of the following options:
   - **Typical install** (Recommended)
   - **Minimal Install**
   - Custom install

   Refer to *Installation Overview* on page 3-2 for the differences.

Note: The default parameters for the Typical and Custom installation are the same.

6. Click **Next**. The **Product Activation** screen appears.

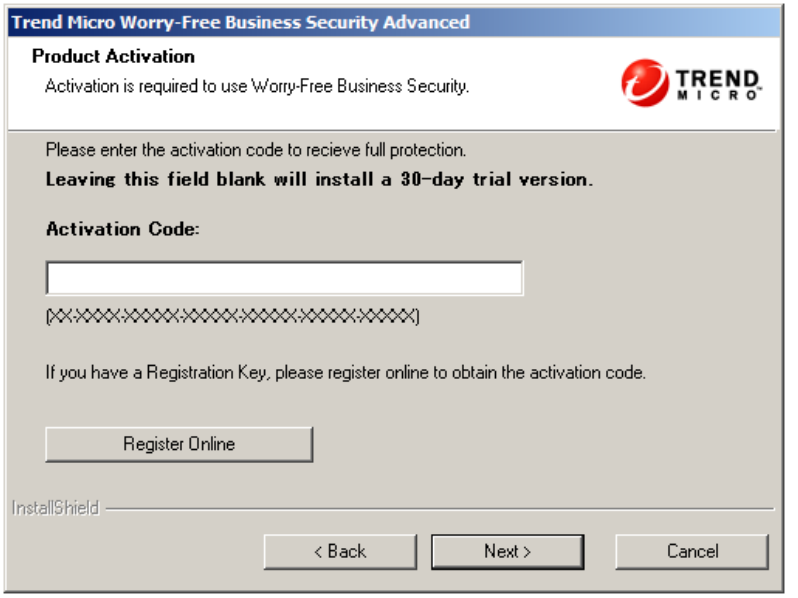


FIGURE 3-2. Product Activation screen

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

Note: 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.

---

8. Click **Next**. The **Setup Overview** screen appears.

FIGURE 3-3. Setup Overview screen

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

9. Click **Next**. The **Select Target Folder** screen appears.

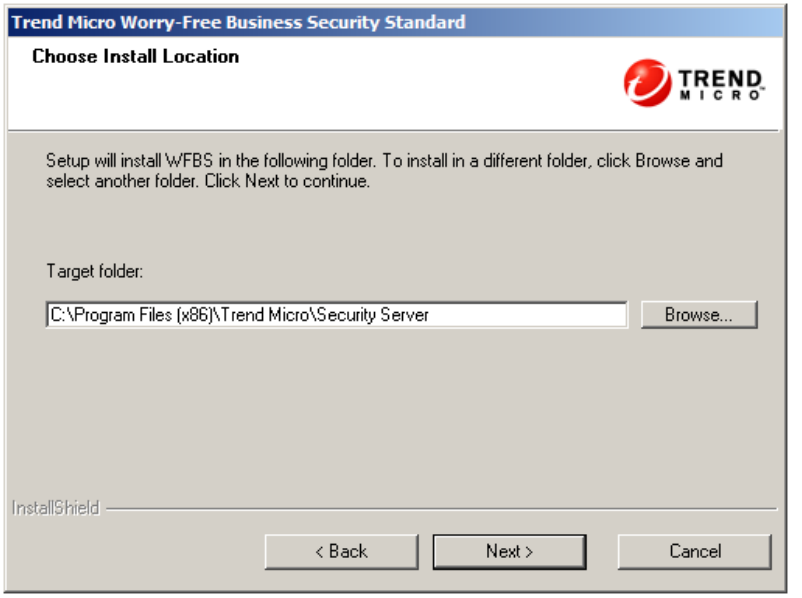


FIGURE 3-4. Select Target Folder screen

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

Note: This screen will not appear if you choose the Typical installation method.

11. Click **Next**. The **Select Components** screen appears.

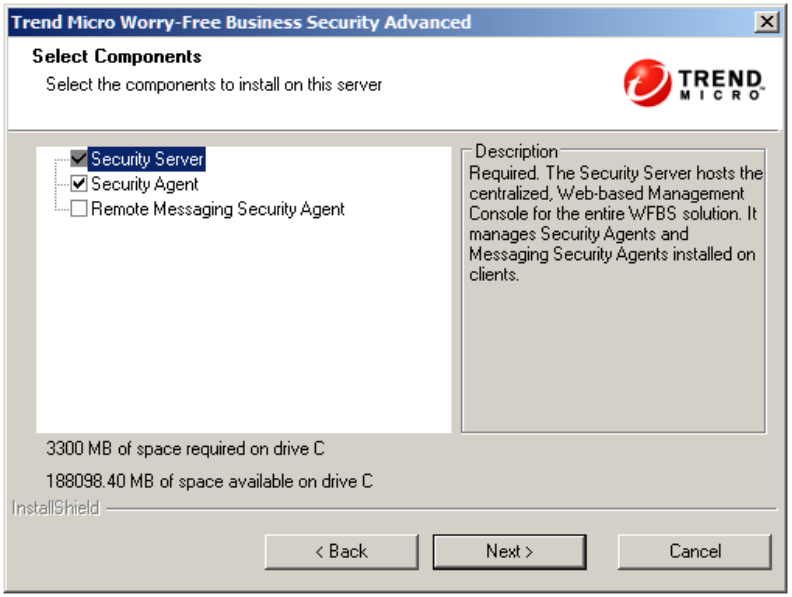


FIGURE 3-5. Select Components screen

12. Select the components that you want to install:
    - **Security Server (default):** The Security Server hosts the centralized Web-based management console
    - **Security Agent (default):** 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

Part 2: Security Server Settings

The Security Server configuration tasks consist prescanning the server for malware, configuring the Web server and the proxy server.

1. The **Configuring Security Server** screen now highlights the Security Server.

FIGURE 3-6. Configure Security Server screen

2. Click **Next**. The **Computer Prescan** screen appears.

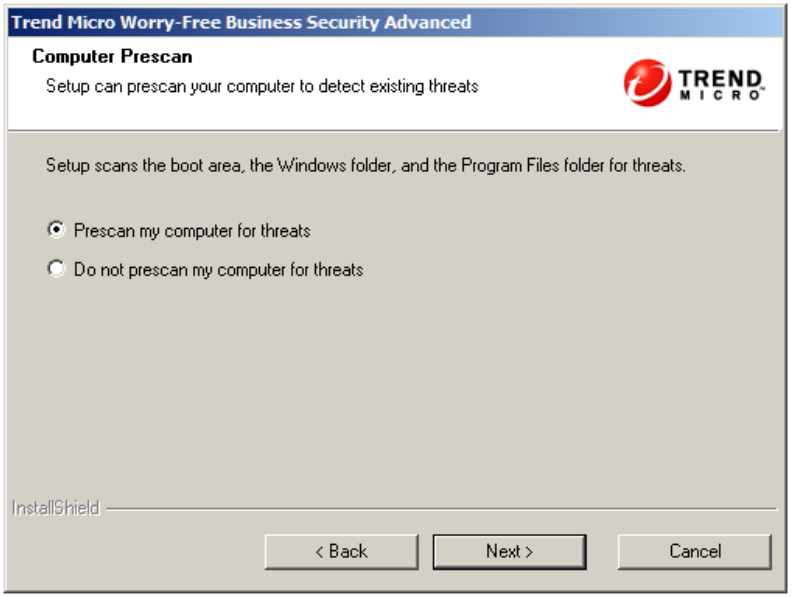


FIGURE 3-7. Computer Prescan screen

3. Choose whether to prescan your computer for threats by selecting one of the following options:
   - **Prescan my computer for threats**: The prescan targets the most vulnerable areas of the computer, which include the following:
     - the Boot area and boot directory (for boot sector viruses)
     - the Windows folder
     - the Program Files folder
   - **Do not prescan my computer for threats**

   Trend Micro highly recommends to prescanning your computer for security threats to ensure that the installation goes into a clean environment. Not prescanning the computer could prevent a successful installation.

4. Click **Next**. The **Web Server** screen appears.

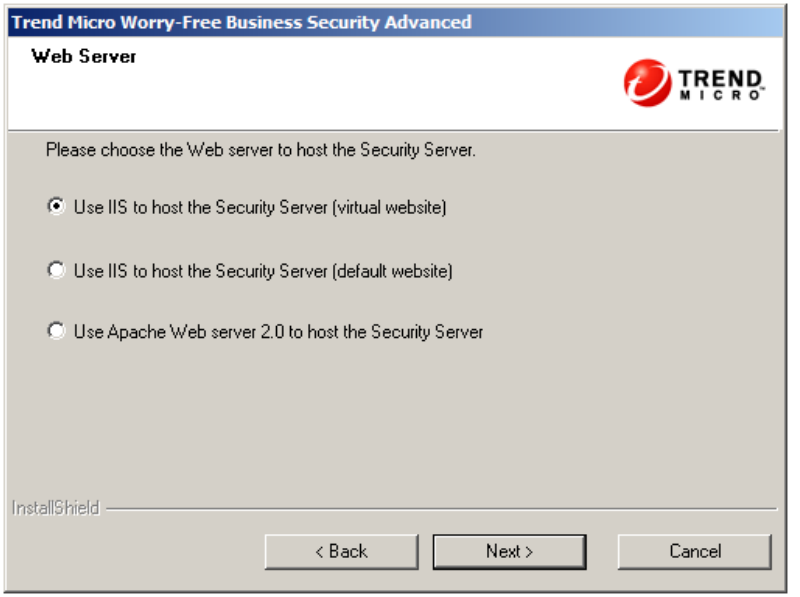


FIGURE 3-8. Web server screen

Note: This screen will not appear if you choose the Typical installation method.

5. From the **Web Server** screen, select a Web server to host the Security Server Web Console. Choose one of the following servers:
   - **Internet Information Services (IIS) server**
   - **Apache Web server 2.0.xx**

6. Click **Next**. The **Web Server Identification** screen appears.

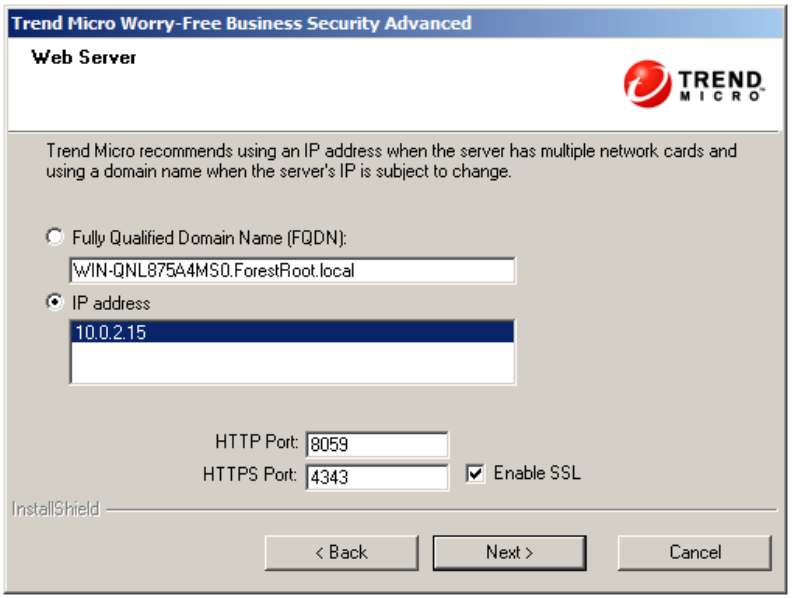


FIGURE 3-9. Web Server Identification screen

7. Choose from one of the following server identification options for client-server communication:
   - **Server information:** Choose domain name or IP address:
     - **Fully Qualified Domain Name:** Use the Web server's domain name to ensure successful client-server communications
     - **IP address:** Verify that the target server's IP address is correct

---

Tip: When using an IP address, ensure that the computer where you are installing the Security Server has a static IP address. If the server has multiple network interface cards (NICs), Trend Micro recommends using the domain name instead of the IP address.

Note: If all access to the Security Server will be done from within your network, you do not need to enable the SSL.

8. Click **Next**. The **Administrator Account Password** screen appears.

FIGURE 3-10. Administrator Account Password screen.

9. The **Administrator Account Password** screen allows you to specify different passwords for the Security Server Web Console and the Security Agent:
   - **Security Server Web Console:** Required to log on the Web Console
     - **Password**
     - **Confirm password**

- **Security Agents:** Required to uninstall Security Agents and remove them from your computer.
  - **Password**
  - **Confirm password**

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

10. Click **Next**. The **SMTP Server and Notification Recipient(s)** screen appears.

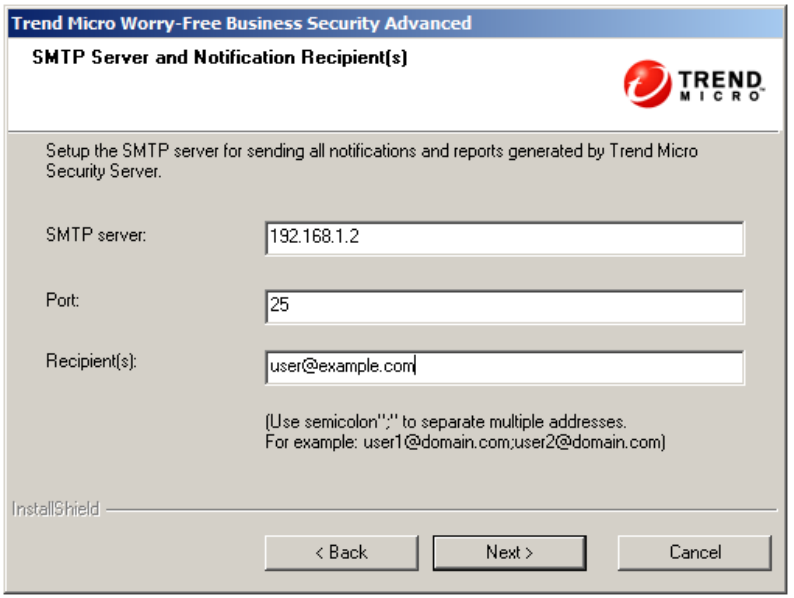


FIGURE 3-11. SMTP Server and Notification Recipient(s) screen

11. The Simple Mail Transfer Protocol (SMTP) Server and Notification Recipient(s) screen requires the following information:
    - **SMTP server**: The IP address of your email server
    - **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

Note: 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.

Tip: 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.

12. Click **Next**. The **Trend Micro Smart Protection Network** screen appears.

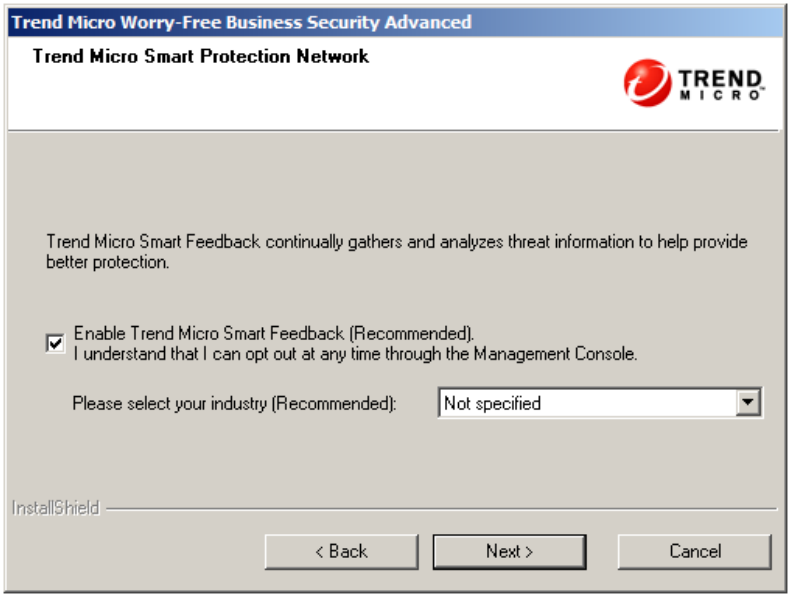


FIGURE 3-12. Trend Micro Smart Protection Network screen

13. 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 that your WFBS 7.0 installation detects. 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 Security Server Web Console later.
14. Click **Next**. The **General Proxy Settings** screen appears.

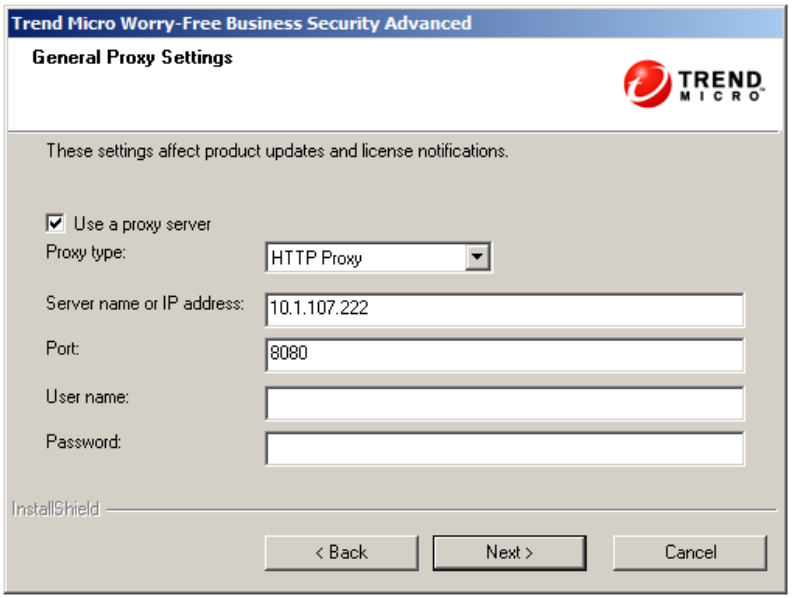


FIGURE 3-13. General Proxy Settings screen

Note: This screen will not appear if you choose the Typical installation method.

15. 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:** To provide only if the proxy server requires authentication

Part 3: Security Agent Installation Options

The Security Agent configuration tasks consist of setting the agent installation path, configuring the agent's server and desktop settings, and the proxy server settings for additional services.

1. The **Configuring Security Agent** screen highlights the Security Agent.

FIGURE 3-14. Configuring Security Agent screen

Note: This screen will not appear if you choose the Typical installation method.

2. Click **Next**. The **Security Agent Installation Path** screen appears.

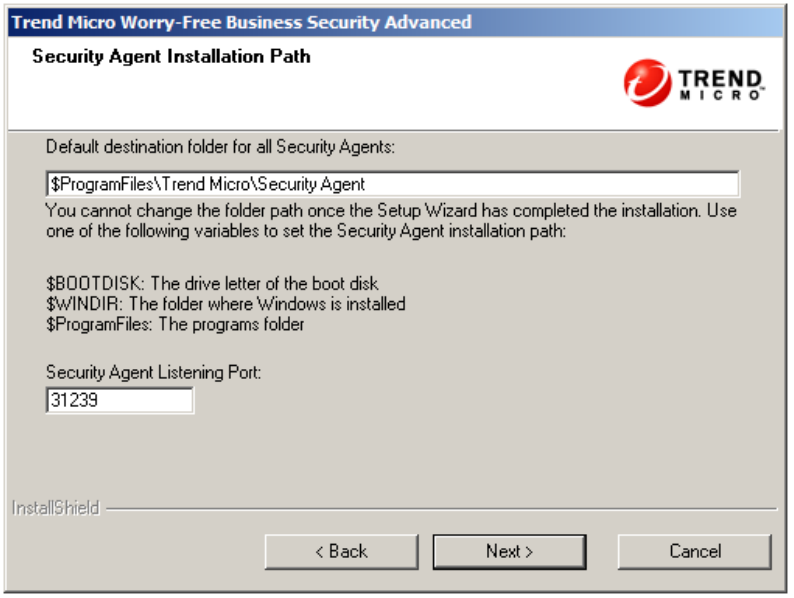


FIGURE 3-15. Security Agent Installation Path screen

Note: This screen will not appear if you choose the Typical installation method.

3. 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

4. Click **Next**. The **Configuring Security Agents Settings** screen appears.

FIGURE 3-16. Configuring Security Agents Settings screen

Note: This screen will not appear if you choose the Typical installation method.

5. You can configure Security Agent settings for Servers and Desktops:
   - **Servers:** Windows Server 2003/2008 computers 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:** Windows XP/Vista/7 computers 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 you 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 of 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
- **Device Control:** Regulates access to external storage devices and network resources

6. Click **Next**. The **Proxy Setting for Additional Services** screen appears.

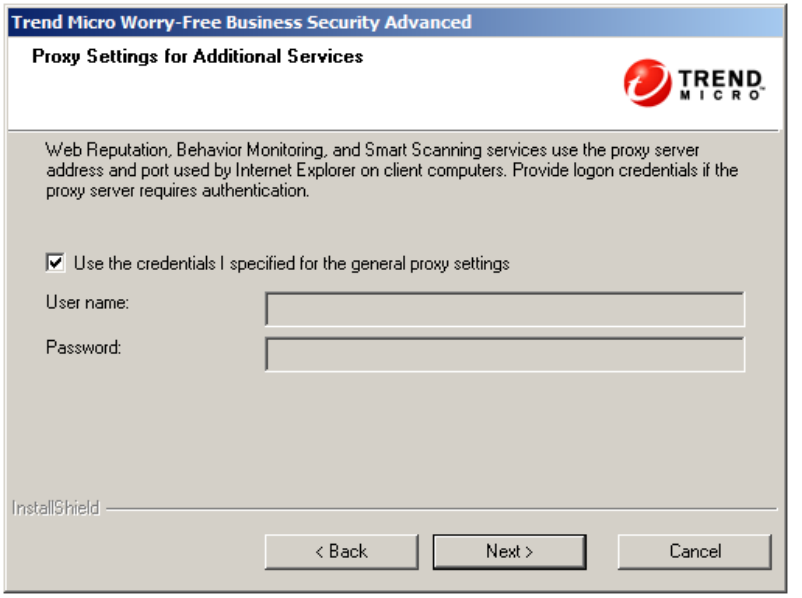


FIGURE 3-17. Proxy Settings for Additional Services screen

Note: This screen will not appear if you choose the Typical installation method.

7. 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.

Part 4: Messaging Security Agent Installation Options

In Worry-Free Business Security Advanced, Messaging Security Agents protect Microsoft Exchange servers. The Messaging Security Agent helps prevent email-borne threats by scanning email passing in and out of the Microsoft Exchange Mailbox Store as well as email that passes between the Microsoft Exchange Server and external destinations.

You can install the Messaging Security Agent using two methods:

Method 1: Install the Messaging Security Agent during the installation of the Security Server. 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.

  Refer to *Figure 3-5. Select Components screen* on page 3-9 for a Security Server components overview.

Method 2: Install the Messaging Security Agent from the Web Console after installation is complete.

To install the Local Messaging Security Agent:

1. The **Configuring Messaging Security Agent** screen highlights the local Messaging Security Agent.

FIGURE 3-18. Configuring Messaging Security Agent screen

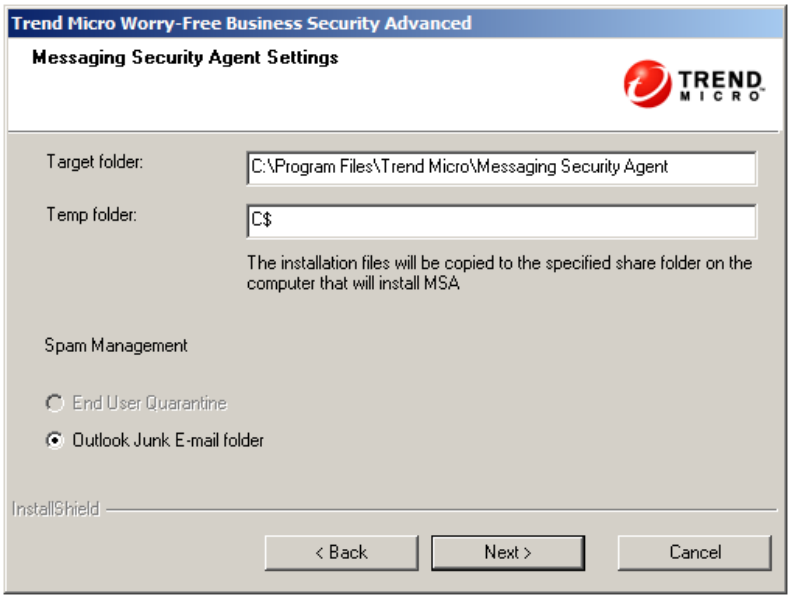
2. Click **Next**. The **Install Messaging Security Agent** screen appears.

FIGURE 3-19. Install Messaging Security Agent screen

3. Provide the following information:
   - **Exchange Server**
   - **Domain Administrator Account**
   - **Password**

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.

4. Click **Next**. The **Messaging Security Agent Settings** screen appears



Note: This screen will not appear if you choose the Typical installation method.

5. In the **Messaging Security Agent Settings** screen, configure the following:
   - **Target Folder:** The folder where the Messaging Security Agent files are installed
   - **Temp Folder:** The system root folder for the Messaging Security Agent installation
   - **Spam management**
     - **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 to select 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. To enable EUQ, read the instructions in this knowledge base article http://esupport.trendmicro.com/pages/How-to-activate-EUQ-in-an-installed-SMEX-10.aspx

To install the Remote Messaging Security Agent:

1. The **Configuring Remote Messaging Security Agent** screen highlights the remote Messaging Security Agent.

FIGURE 3-20. Configuring Remote Messaging Security Agent Screen

2. Click **Next**. The **Install Remote Messaging Security Agent** screen appears.

FIGURE 3-21. Install Remote Messaging Security Agent screen

3. Provide the following information:
   - **Exchange Server:** IP address or computer name
   - **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 workaround this issue, either temporarily change the password to the built-in domain administrator account or install the Messaging Security Agent directly on the Exchange server.

4. Click **Next**. The **Remote Messaging Security Agent Settings** screen appears.

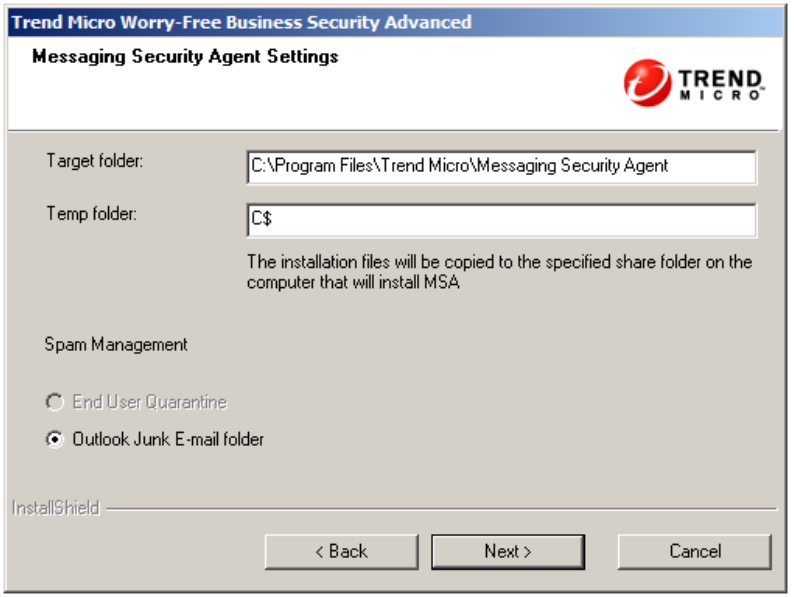


FIGURE 3-22. Remote Messaging Security Agent Settings screen

Note: This screen will not appear if you choose the Typical installation method.

5. In the **Remote Messaging Security Agent Settings** screen, configure the following:
   - **Target Folder:** The folder where the Remote Messaging Security Agent files are installed
   - **Temp Folder:** The system root folder for the Remote Messaging Security Agent installation
   - **Spam management**
     - **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 to select 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. To enable EUQ, read the instructions in this knowledge base article http://esupport.trendmicro.com/pages/How-to-activate-EUQ-in-an-installed-SMEX-10.aspx

---

6. Click **Next**. The program begins installing the Remote Messaging Security Agent on the remote Exchange server.
7. Upon completion, the **Remote Messaging Security Agent Status** screen re-appears. Repeat the above process to install the Remote Messaging Security Agents on other Exchange servers.

Part 5: Installation Process

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

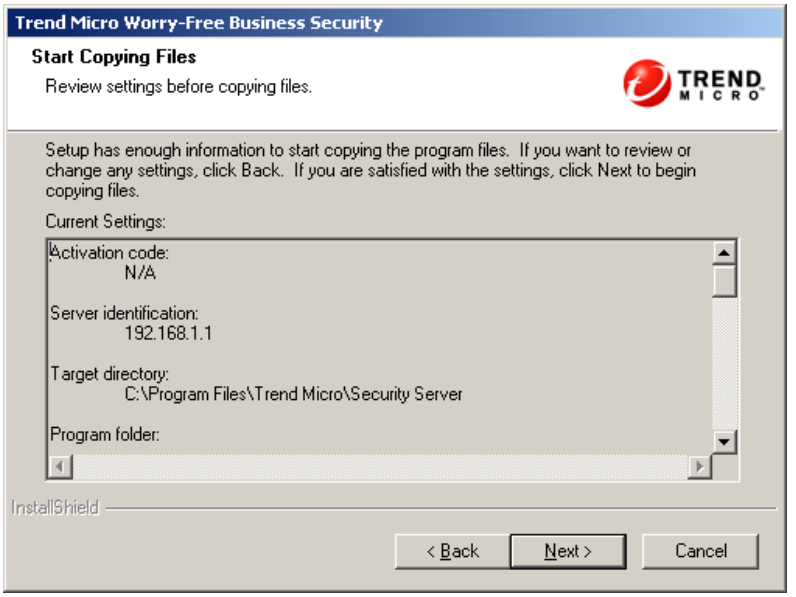


FIGURE 3-23. Start Copying Files screen

1. Click **Back** if you wish to verify previous installation settings, or click **Next** to proceed with the actual installation. The **Install Third Party Components** screen appears.

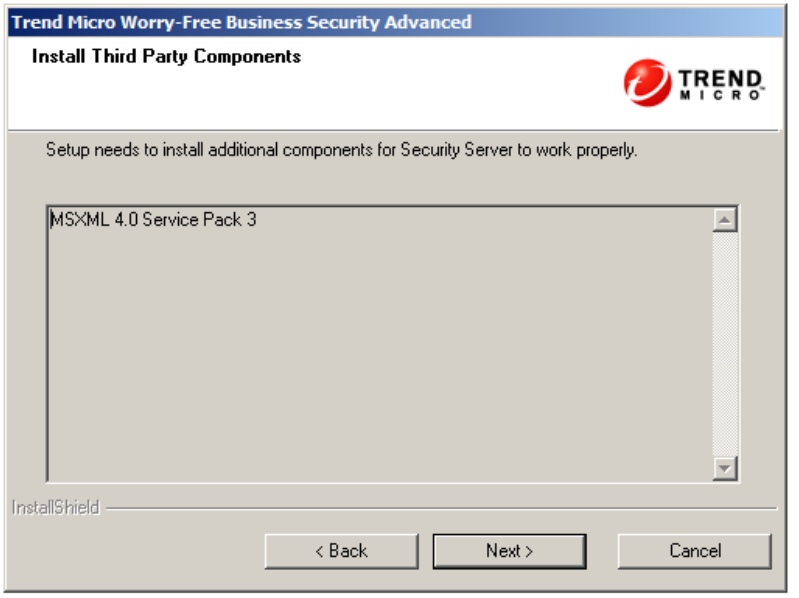


FIGURE 3-24. Install Third Party Components screen

2. This screen informs you which third party components will be installed. Click **Next** to start installing the selected components. The entire installation process may take some time to complete. During the installation, a status screen will show the progress being made.
3. Once setup is complete, the **Setup Wizard Complete screen** appears. Click **Finish** to close the install procedure.

Silent Installation Walkthrough

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.

To record an installation session:

1. Download and extract the WFBS 7.0 files on your hard disk. When the Setup Wizard starts with collecting installation settings, click **Cancel** > **Yes** > **Finish**.

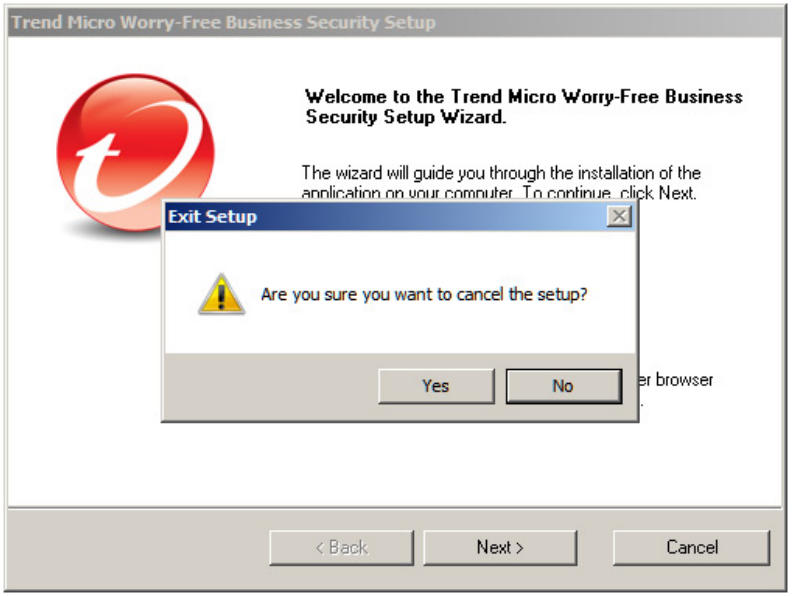


FIGURE 3-25. Interrupt the Setup Wizard to Start the Recording Session

2. In **command prompt mode**, navigate to the directory where the extracted WFBS setup files are located, for example: `C:\Extract\WBS70\CSM`
3. At the prompt, type `Setup.exe /r /f1"c:\silent-install.iss"`. 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 *Typical Installation Walkthrough* on page 3-3 and *Custom Installation Walkthrough* on page 3-3
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.

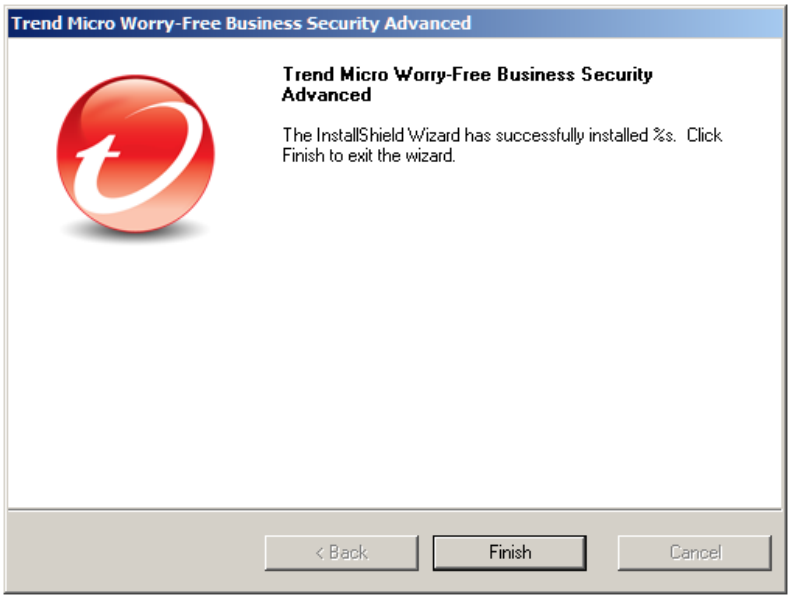


FIGURE 3-26. Click Finish to End the Recording Session

Starting the silent installation:

1. In **command prompt mode**, navigate to the directory where the extracted WFBS setup files are located, for example: `C:\Extract\WBS70\CSM`
2. At the prompt, type `Setup.exe /s /f1"c:\silent-install.iss"`. Click **Enter**.

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

   Note: During Silent installation, no progess indicators will be shown on your screen.

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

Verifying the Installation

Alternatively, you can verify if the WFBS Security Server and Agents are properly installed:

To verify the installation:

- Click **Start** > **All Programs** to see if the WFBS program 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.

Installing the Trend Micro Worry-Free Remote Manager Agent

If you are a Trend Micro certified partner, you can install the agent for Trend Micro™ Worry-Free™ Remote Manager (WFRM). If you chose not to install the WFRM agent after the Security Server installation completes, you can do so later.

Before starting the installation, ensure that you have the WFRM Agent GUID. To obtain the GUID, open the WFRM Console and go to:

Customers (tab) **> All Customers** (on the tree) **>** {customer} > WFBS**/CSM** > **Server/Agent Details** (right pane) > **WFRM Agent Details**

The installation requires the following pre-requisites:

- An active Internet connection
- 50MB of free disk space

To install the agent with the installation file:

1. Go to the Security Server and navigate to the following installation folder: `PCCSRV\Admin\Utility\RmAgent`, and launch the application `WFRMforWFBS.exe`.

   For example:

   ```
   C:\Program Files\Trend Micro\Security
   Server\PCCSRV\Admin\Utility\RmAgent\WFRMforWFBS.exe
   ```

2. In the **Worry-Free Remote Manager Agent** Setup Wizard, click **Yes** to confirm that you are a certified partner.
3. Select **I already have a Worry-Free Remote Manager account and I want to install the agent**. Click **Next**.
4. If this is a **new** customer:
   a. Select **Associate with a new customer**
   b. Click **Next**. Enter the customer information
   c. Click **Next**. Select the **Region** and **Protocol**, and enter the **Proxy** information if required Click **Next**.

WARNING! **If the customer already exists on the WFRM Console and you use the option above to associate with a new customer, this will result in two duplicate customers with the same name appearing on the WFRM network tree. To avoid this, use the method below:**

If this is an **existing** customer:

a. Select **This product already exists in Remote Manager**

WFBS must already have been added to the WFRM Console. See your WFRM documentation for instructions.

b. Type the GUID

5. Click **Next**. Select the **Region** and **Protocol**, and enter the **Proxy** information if required.
6. Click **Next**. The **Installation Location** screen opens.
7. To use the default location, click **Next**.
8. Click **Finish**.

If the installation is successful and settings are correct, the WFRM Agent should automatically register to the Worry-Free Remote Manager server. The Agent should show as Online on the WFRM Console.

Chapter 4

Upgrading and Migrating

This chapter provides information you will need to understand to upgrade from previous versions of Worry-Free Business Security (WFBS).

The topics discussed in this chapter include:

Upgrading from a Previous Version

The upgrade procedure is similar to the normal installation process except you type your existing Security Server when asked to identify the Security Server (domain name or IP address). Security Agents and Messaging Security Agents will upgrade automatically.

Note: All previous settings will be retained after upgrading to this version 7.0.

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

TABLE 4-1. Product Versions

Product Version	Worry-Free Business Security	Worry-Free Business Security Advanced
Client-side solution	Yes	Yes
Server-side solution	Yes	Yes
Exchange-server solution	No	Yes

You can upgrade from Worry-Free Business Security to Worry-Free Business Security Advanced by typing the appropriate Activation Code in the **Product License** screen of the Web Console.

Supported Upgrades

WFBS 7.0 supports upgrades from any of the following versions:

- Upgrade from Worry-Free Business Security or Worry-Free Business Security Advanced versions 5.0, 5.1, and 6.0.

Unsupported Upgrades

WFBS 7.0 does not support upgrades from the following program versions:

- All upgrades that supported Windows 2000
- Upgrade form Client/Server Messaging Security 3.6
- Upgrade from Client/Server Messaging Security 3.5
- Upgrade from Client/Server/Messaging Security 3.0
- Upgrade from Client/Server Security 3.0
- Upgrade from Client/Server Suite 2.0
- Upgrade from Client/Server/Messaging Suite 2.0
- Upgrade from OfficeScan or ScanMail for Microsoft Exchange
- Upgrade from one language to another

Upgrading 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 backing up your Security Server database.

To back up the Security Server database:

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).

Trend Micro recommends deleting all log files from the Security Server before upgrading.

To delete log files:

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.

Upgrading Walkthrough

When your evaluation version is about to expire, a notification message displays on the **Live Status** screen on the WFBS 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.

To upgrade from an evaluation version:

1. Open the WFBS Web Console.
2. On the main menu, under **License**, click **view Product License details**. The **License Information** screen appears.
3. If you have an Activation Code, click **Enter a new code**, type it in the **New Activation Code** field, and click **Activate**.

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

Migrating from Other Anti-Malware Applications

WFBS 7.0 supports migration from other anti-malware applications.

Note: WFBS 7.0 can automatically migrate the client software, but cannot uninstall the server application.

Migrating from antivirus software to WFBS is a two-step process: the installation of the Trend Micro Security Server, followed by the automatic migration of the clients. Automatic client migration refers to replacing existing client antivirus software with the

Security Agent program. The client setup program automatically removes the other antivirus software on your client computers and replaces it with the Security Agent. Refer to *Table 4-2* for a list of client applications that WFBS can automatically remove.

Note: WFBS only removes the following client installations, not server installations.

TABLE 4-2. Removable Antivirus Applications

TREND MICRO™		
Trend Micro Internet Security 2008/2009/2010 Trend Micro Internet Security Pro 2008/2009/2010 Trend Micro Titanium 1.0 Trend Micro Titanium 2.2/3.0	Worry-Free Business Security Service 2.5/3.0 Trend Micro OfficeScan 8.0/10.0/10.5	
SYMANTEC™		
Norton Antivirus CE 8.0 9x Norton Antivirus CE 8.0 NT Norton Antivirus CE 8.1 server Norton Antivirus CE 9.0 Norton Antivirus CE 10.0 Norton Antivirus CE 10.1	Norton AntiVirus 2008/2009/2010 Symantec Internet Security 2008/2009/2010 Norton 360 v200 Symantec Endpoint Protection 11/12 Symantec AntiVirus 10/11/12 Symantec Client Security 10/11/12	

TABLE 4-2. Removable Antivirus Applications (Continued)

MCAFEE™		
McAfee VirusScan ASaP McAfee VirusScan ASaP Mcafee Managed VirusScan McAfee SpamKiller McAfee SecurityCenter 7	McAfee VirusScan Enterprise 7 McAfee VirusScan NT McAfee VirusScan Enterprise 7/8/8.5/8.7 McAfee Anti-Spyware Enterprise 8.0 McAfee Desktop Firewall 8.0 McAfee Internet Security 2009 McAfee VirusScan Professional 9.0	
LANDESK™		
LANDesk VirusProtect5.0		
COMPUTER ASSOCIATES™		
CA InocuLAN 5 CA eTrust InoculateIT 6.0/7.0/7.1	CA eTrustITM 8.0/8.1 CA iTechnology iGateway 4.0/4.2	
AHNLAB™		
V3Pro 2000 Deluxe	V3Pro 98 Deluxe	
PANDA SOFTWARE™		

TABLE 4-2. Removable Antivirus Applications (Continued)

Panda Antivirus Local Networks	Panda Antivirus 6.0	Panda Antivirus Windows NT WS Panda Platinum Internet Security 2004/2005 Panda Platinum 7.0 Panda Titanium Antivirus 2007
F-SECURE™		
F-Secure 4.04 F-Secure 4.08, 4.3 5.3	F-Secure BackWeb F-Secure Client Security 7.10 - E-mail Scanning F-Secure Client Security 7.10 - System Control F-Secure Client Security 7.10 - Internet Shield F-Secure Client Security 7.10 - Web Traffic Scanning	F-Secure Management Agent F-Secure Anti-Virus 2008 F-Secure Internet Security 2008 F-Secure Anti-Virus for Workstations 7.11 F-Secure Anti-Virus for Workstations 8.00
KASPERSKY™		
Kaspersky Internet Security 2009/2010 Kaspersky Anti-virus 6.0 Kaspersky Internet Security 7.0		
MICROSOFT™		
Microsoft Forefront Client Security Antimalware Service 1.0/1.5 Microsoft Forefront Client Security State Assessment Service 1.0 Microsoft OneCare 2.x		

TABLE 4-2. Removable Antivirus Applications (Continued)

SOPHOS™		
Sophos Anti-Virus 9X Sophos Anti-Virus NT 5.0/7.0 Sophos Anti-Virus NT 7.0		
AUTHENTIUM™		
Command AV 4.64 9x		
AMREIN™		
Cheyenne AntiVirus 9X	Cheyenne AntiVirus NT	
GRISOFT™		
Grisoft AVG 6.0/7.0 AVG Free 8.5/9.0		
OTHERS		
ViRobot 2k Professional	Tegam ViGUARD 9.25e for Windows NT	

Upgrading the Security Agent

You can upgrade to a full version of from a previous version or from an evaluation version. When you upgrade the Trend Micro Security Server, the Security Agents in your network are automatically upgraded as well.

Preventing Upgrade for Selected Clients

Upgrading a large number of clients simultaneously can significantly increase network traffic. WFBS provides an option to prevent selected clients from upgrading to the current version. If there are a large number of clients to be upgraded, Trend Micro recommends disabling program update for certain groups of clients before upgrade, and then upgrading them later.

To disable program update:

1. On the WFBS Web Console, select **Security Settings > Select a group > Configure > Client Privileges**.
2. Under Update Settings, select **Disable program upgrade and hot fix deployment** and save your settings.

   Note: These clients will not be upgraded to the next version, but will still receive component updates (such as the malware/virus pattern files) to keep their protection up to date.

3. When ready to upgrade these clients, clear the same check box, save your settings, and perform agent installation for these clients using the installation method of your choice.

Chapter 5

Getting Started

This chapter tells you how to get WFBS up and running. Topics discussed in this chapter include:

Registering

You need to register and activate your product to enable pattern file and scan engine updates. When you purchase the product, you will receive licensing and registration information from Trend Micro, including a Registration Key that you must use during the product registration process.

During the installation, the installation program will prompt you to enter your Registration Key and Activation Code. If you do not have a Registration Key, contact your Trend Micro sales representative. If you do not have the Activation Code(s), use the Registration Key that came with your product to register on the Trend Micro website and receive the Activation Code(s).

A Registration Key is 37characters in length, including hyphens, in the following format:

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

Most Trend Micro products use a Registration Key. When you are ready to register, go to the following Trend Micro website:

http://olr.trendmicro.com

Introducing the Web Console

The Web Console is a centralized Web-based management console. You can use it to configure all agents from a Web browser connected through a network to any of your protected computers. The Worry-Free Business Security Advanced Web Console is installed when you install the Trend Micro Security Server and uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

Use the following menu options from Web Console:

- **Live Status:** provides a central function in the Worry-Free Business Security strategy. Use Live Status to view alerts and notifications about outbreaks and critical security risks.
    - View red or yellow alert warnings issued by Trend Micro
    - View the latest threats to desktops and servers on your network
    - View the latest threats to Microsoft Exchange servers (Advanced only)
    - Deploy updates to clients that are at risk

- **Security Settings:**
  - Customize security settings for the Security Agent
  - Customize security settings for Microsoft Exchange servers
  - Replicate settings from one group of clients to another group of clients
- **Outbreak Defense:** provides alerts to current status and guides you through an outbreak cycle.
- **Scans:**
  - Scan clients for viruses and other malware
  - Schedule scanning for clients
  - Vulnerability Assessment
- **Updates:**
  - Checks the Trend Micro ActiveUpdate server for the latest updated components, including updates to the virus pattern, scan engine, Cleanup components, and the program itself
  - Configure update source
  - Designate Security Agents as Update Agents
- **Reports**
- **Preferences:**
  - Set up notifications for abnormal threat-related or system-related events
  - Set up global settings for ease of maintenance
  - Use Client and Administrative tools to help manage security for the network and clients
  - View product license information, maintain the administrator password, and help keep the business environment safe for the exchange of digital information by joining the World Virus Tracking program
- **Help**

The console contains the following, main sections:

TABLE 5-1. Web Console Main Features

FEATURE	DESCRIPTION
Main menu	Along the top of the Web Console is the main menu. This menu is always available.
Configuration area	Below the main menu items is the configuration area. Use this area to select options according to the menu item you selected.
Menu sidebar	When you choose a client or group from the **Security Settings** screen and click **Configure**, a menu sidebar displays. Use the sidebar to configure security settings and scans for your desktops and servers. When you choose a Microsoft Exchange server from the **Security Settings** screen (Advanced only), you can use the sidebar to configure security settings and scans for your Microsoft Exchange servers.
Security Settings toolbar	When you open the **Security Settings** screen, you can see a toolbar containing a number of icons. When you click a client or group from the **Security Settings** screen and click an icon on the toolbar, the Security Server performs the associated task.

To open the Web Console:

1. Select one of the following options to open the Web Console:
   - Click the **Worry-Free Business Security** shortcut on the Desktop.
   - From the Windows™ Start menu, click **Trend Micro Worry-Free Business Security > Worry-Free Business Security**.
   - You can also open the Web Console from any computer on the network. Open a Web browser and type the following in the address bar:

     `https://{Security_Server_Name}:{port number}/SMB`

     For example:

     `https://my-test-server:4343/SMB`

     `https://192.168.0.10:4343/SMB`

`http://my-test-server:8059/SMB`

`http://192.168.0.10:8059/SMB`

If you are NOT using SSL, type `http` instead of `https`. The default port for HTTP connections is 8059 and for HTTPS connections is 4343.

Tip: If the environment cannot resolve server names by DNS, replace {Security_Server_Name} with {Server_IP_Address}.

2. The browser displays the **Trend Micro Worry-Free Business Security logon** screen.

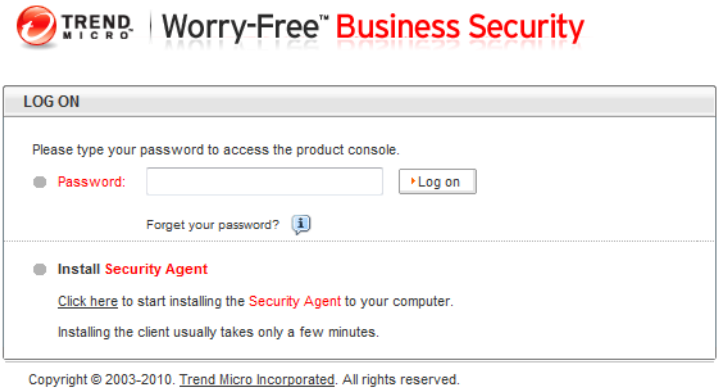


FIGURE 5-1. Logon screen of WFBS

3. Type your password and click **Log on**. The browser displays the **Live Status** screen.

Web Console Icons

The table below describes the icons displayed on the Web Console and explains what they are used for.

TABLE 5-2. Web Console Icons

ICON	DESCRIPTION
	**Help** icon. Opens the online help.
	**Refresh** icon. Refreshes the view of current screen.
	**Expand/Collapse section** icon. Displays/hides sections. You can expand only one section at a time.
	**Information** icon. Displays information pertaining to a specific item.

Live Status

Use the Live Status screen to manage WFBS.

The refresh rate for information displayed on the Live Status screen varies per section. In general, the refresh rate is between 1 to 10 minutes. To manually refresh the screen information, click **Refresh**.

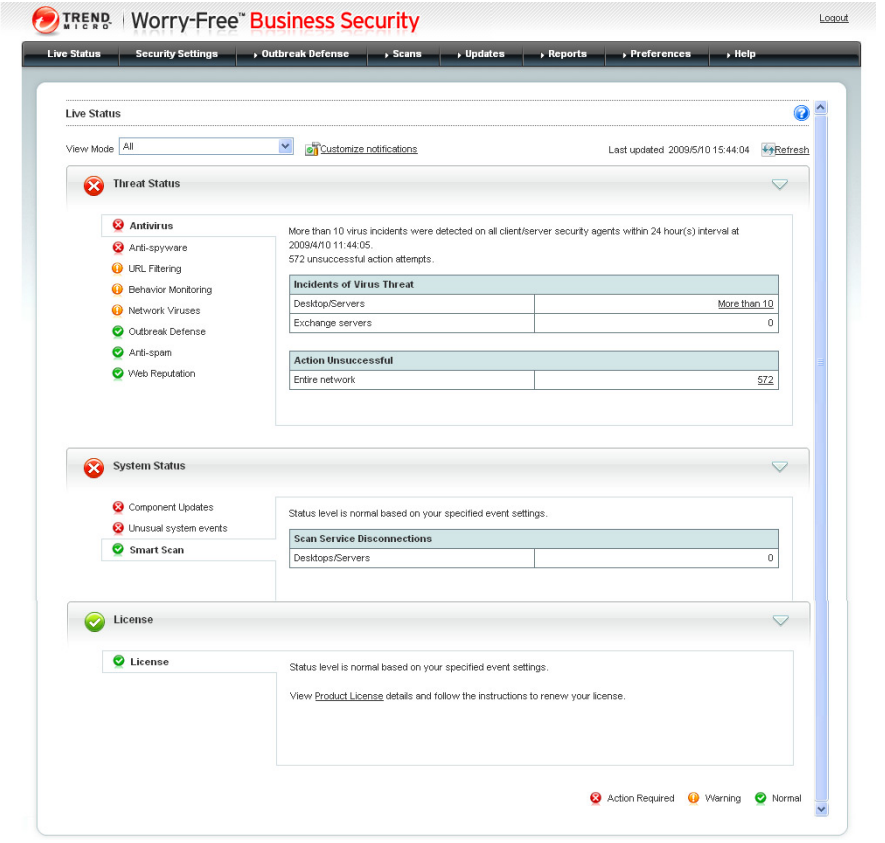


FIGURE 5-2. Worry-Free Business Security Live Status screen

Understanding Icons

Icons warn you if any action is necessary. Expand a section to view more information. You can also click the items in the table to view specific details. To find more information about specific clients, click the number links that appear in the tables.

TABLE 5-3. Live Status Icons

ICON	DESCRIPTION
	Normal Only a few clients require patching. The virus, spyware, and other malware activity on your computers and network represents an insignificant risk.
	Warning Take action to prevent further risk to your network. Typically, a warning icon means that you have a number of vulnerable computers that are reporting too many virus or other malware incidents. When a Yellow Alert is issued by Trend Micro, the warning displays for Outbreak Defense.
	Action required A warning icon means that the administrator must take action to solve a security issue.

The information displayed on the Live Status screen is generated by the Security Server and based on data collected from clients.

Threat Status

Displays information about the following:

- **Antivirus:** starting from the 5th incident, the status icon changes to display the Warning. If you must take action:
  - The Security Agent did not successfully perform the action it was set up to perform. Click the numbered link to view detailed information about computers on which the Security Agent was unable to perform and take an action.

  - Real-time scanning is disabled on Security Agents. Click **Enable Now** to start Real-time scanning again.
  - The real-time scanning is disabled on the Messaging Security Agent.
- **Anti-spyware:** displays the latest spyware scan results and spyware log entries. The Number of Incidents column of the Spyware Threat Incidents table displays the results of the latest spyware scan.
  - To find more information about specific clients, click the number link under the **Incidents Detected** column of the Spyware Threat Incidents table. From there, you can find information about the specific spyware threats that are affecting your clients.
- **URL Filtering:** restricted websites as determined by the administrator. Starting from the 300th incident, the status icon changes to display a warning.
- **Behavior Monitoring:** violations of the behavior monitoring policies.
- **Network Viruses:** detections determined by the firewall settings.
- **Outbreak Defense:** a possible virus outbreak on your network.
- **Anti-spam:** click the **High**, **Medium**, or **Low** link to be redirected to the configuration screen for the selected Microsoft Exchange server where you can set the threshold level from the Anti-spam screen. Click **Disabled** to be redirected to the appropriate screen. This information is updated on an hourly basis.
- **Web Reputation:** potentially dangerous websites as determined by Trend Micro. Starting from the 200th incident, the status icon changes to display a warning.
- **Device Control:** restricts access to USB devices and network drives

System Status

Information regarding the updated components and free space on computers where Agents are installed.

- **Component Updates:** the status of component updates for the Security Server or the deployment of updated components to Agents.
- **Unusual system events:** disk space information about clients that are functioning as servers (running server operating systems).

- **Smart Scan:** the clients that cannot connect to their assigned scan server.

> **Tip:** You can customize the parameters that trigger the Web Console to display a Warning or Action Required icon from **Preferences > Notifications**.

License Status

Information regarding the license status.

- **License:** information about the status of your product license, specifically expiration information.

Live Status Update Intervals

To understand how often Live Status information will be updated, see the following table.

TABLE 5-4. Live Status Update Intervals

ITEM	UPDATE INTERVAL (MINUTES)	AGENT SENDS LOGS TO SERVER AFTER... (MINUTES)
Outbreak Defense	3	N/A
Antivirus	1	SA: Immediate MSA: 5
Anti-spyware	3	1
Anti-spam	3	60
Web Reputation	3	Immediate
URL Filtering	3	Immediate
Behavior Monitoring	3	2
Network Virus	3	2
Smart Scan	60	N/A
License	10	N/A

TABLE 5-4. Live Status Update Intervals (Continued)

ITEM	UPDATE INTERVAL (MINUTES)	AGENT SENDS LOGS TO SERVER AFTER... (MINUTES)
Component Updates	3	N/A
Unusual System Events	10	When the listening service TmListen is started
Device Control	3	2

Viewing Computers

Navigation Path: Security Settings {tab}

The Security Settings screen allows you to manage all the computers on which you installed Agents. When you select a group from the Security Groups Tree, the computers in that group display in a table to the right.

The Security Settings screen is divided into two (2) main sections:

Global Navigation Menu

These menu items are always available.

Configuration Area

The configuration area includes the Security Server information bar, the configuration toolbar, and below the toolbar, the Security Groups Tree and Security Agent information table.

Security Server information bar: Displays information about the Security Server such as Domain name, port number, and number of desktops and servers managed.

Toolbar:

- **Configure:** The Configure tool is only available when one of the items in the Security Groups Tree is selected. The Configure tool allows you to configure settings for all Agents within that group. All computers in a group must share the same configuration. You can configure the following:

Scan method (Smart or Conventional), Antivirus/Anti-spyware, Firewall, Web Reputation, URL Filtering, Behavior Monitoring, Device Control, User Tools, Client Privileges, and Quarantine

Note: (Advanced only) If you are using Internet Explorer 8 and you click **Configure** for a Messaging Security Agent, a message appears asking you if you want to view only secure Web page content. You must click **No** to view the MSA settings page.

- **Replicate Settings:** The Replicate Settings tool is only available when one of the items in the Security Groups Tree is selected and there is at least one other item of the same type in the Security Groups Tree.
- **Import/Export Settings:** Save your configuration settings or import settings that you have already saved.
- **Add Group:** The Add Group tool allows you to add new desktop or server groups.
- **Add:** The Add tool allows you to add computers to specific groups by deploying Security Agents to computers you specify.
- **Remove:** The Remove tool will remove the Agent from the computers that you specify.
- **Move:** The Move tool allows you to move selected computer or servers from one Security Server to another.
- **Reset Counters:** The Reset Counters tool works on all computers within a group. When clicked, the value in the Viruses Detected and Spyware Detected columns of the Security Agent information table will be reset to zero.
- **Security Groups Tree:** Select a group from the Security Groups Tree to display a list of computers in that group to the right.
- **Security Agent information table:** When you select a client and click a tool from the toolbar, the Web Console displays a new configurations area.

Key Components

The following are the major, key components of Worry-Free™ Business Security:

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 a client-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 Security Agents.

The Security Server performs these important functions:

- Installs, monitors, and manages Agents on the network
- Downloads virus pattern files, Spyware/Grayware Pattern v.6 files, scan engines, and program updates from the Trend Micro update server, and then distributes them to Agents

Security Agent

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

The Security Agent provides three methods of scanning: Real-time Scan, Scheduled Scan, Manual Scan.

Configure scan settings on Agents from the Web Console. To enforce uniform desktop protection across the network, choose not to grant users privileges to modify the scan settings or to remove the Agent.

Web Console

The Web Console is a centralized, Web-based, management console. Use the Web Console to configure Agents. The Web Console is installed when you install the Trend Micro Security Server and uses Internet technologies such as ActiveX, CGI, HTML, and HTTP/HTTPS.

Also use the Web Console to:

- Deploy the Agents to servers, desktops, and portable computers.
- Combine desktops and portable computers and servers into logical groups for simultaneous configuration and management.
- Set antivirus and anti-spyware scan configurations and start Manual Scan on a single group or on multiple groups.
- Receive notifications and view log reports for virus activities.
- Receive notifications and send outbreak alerts through email messages, SNMP Trap, or Windows Event Log when threats are detected on Clients.

Control outbreaks by configuring and enabling Outbreak Prevention.

Clients

Clients are all the desktops, laptops, and servers where the Security Agent (SA) is installed. Microsoft Exchange servers protected by Messaging Security Agents (MSA) (Advanced only) are also considered to be Clients. SAs perform virus and spyware scanning and Firewall configurations on Clients. MSAs (Advanced only) perform virus scanning, spam filtering, email content filtering, and attachment blocking on Microsoft Exchange servers.

Virus Scan Engine

At the heart of all Trend Micro products lies a scan engine. Originally developed in response to early file-based computer viruses, the scan engine today is exceptionally sophisticated and capable of detecting Internet worms, mass mailers, Trojan horse threats, phishing sites, and network exploits as well as viruses. The scan engine detects two types of threats:

- Actively circulating: Threats that are actively circulating on the Internet

- Known and controlled: Controlled viruses not in circulation, but that are developed and used for research

Rather than scan every byte of every file, the engine and pattern file work together to identify not only tell-tale characteristics of the virus code, but the precise location within a file where a virus would hide. If Worry-Free Business Security detects a virus, it can remove it and restore the integrity of the file. The scan engine receives incrementally updated pattern files (to reduce bandwidth) from Trend Micro.

The scan engine is able to decrypt all major encryption formats (including MIME and BinHex). It recognizes and scans common compression formats, including ZIP, ARJ, and CAB. If Worry-Free Business Security can also scan multiple layers of compression within a file (maximum of six).

It is important that the scan engine remain current with new threats. Trend Micro ensures this in two ways:

- Frequent updates to the virus pattern file
- Upgrades to the engine software prompted by a change in the nature of virus threats, such as a rise in mixed threats like SQL Slammer

The Trend Micro scan engine is certified annually by international computer security organizations, including ICSA (International Computer Security Association)

Scan Engine Updates

By storing the most time-sensitive virus information in the virus pattern file, Trend Micro is able to minimize the number of scan engine updates while at the same time keeping protection updated. Nevertheless, Trend Micro periodically makes new scan engine versions available. Trend Micro releases new engines under the following circumstances:

- New scanning and detection technologies are incorporated into the software
- A new, potentially harmful virus is discovered
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit the Trend Micro website:

http://www.trendmicro.com

Chapter 6

Managing Basic Security Settings

This chapter explains how to configure basic security settings. Topics discussed in this chapter include:

Options for Desktop and Server Groups

In WFBS, Groups are a collection of clients that share the same configuration and run the same tasks. By grouping clients, you simultaneously configure and manage multiple clients. See *Groups* on page 4-2.

The following items can be accessed by selecting a group from the **Security Settings** screen and clicking **Configure**:

TABLE 6-1. Configuration Options for Desktop and Server Groups

OPTION	DESCRIPTION	DEFAULT
Scan Method	Configure whether Smart Scan is enabled or disabled.	Enabled or Disabled is chosen during WFBS installation.
Antivirus/Anti-spyware	Configure Real-time Scan, antivirus, and anti-spyware options	Enabled (Real-time Scan)
Firewall	Configure Firewall options	Disabled
Web Reputation	Configure In Office and Out of Office Web Reputation options	In Office: Enabled, Low Out of Office: Enabled, Medium
URL Filtering	URL filtering blocks websites that violate configured policies.	Enabled
Behavior Monitoring	Configure Behavior Monitoring options	Enabled for Desktop Groups Disabled for Server Groups
Device Control	Configure Autorun and USB and network access	Disabled
User Tools	Configure Transaction Protector (Wi-Fi Advisor), Trend Protect (Page Ratings), and Trend Micro Anti-spam Toolbar	Disabled: Wi-Fi Advisor Disabled: Page Ratings Disabled: Anti-spam Toolbar in supported email clients
Client Privileges	Configure access to settings from the client console	N/A
Quarantine	Specify the Quarantine directory	N/A

Note: Other client settings apply to all clients and are accessible through the **Desktop/Server** tab on the **Preferences > Global Settings** screen.

Configuring Real-time Scan

Navigation Path: Security Settings > {group} **> Configure > Antivirus/Anti-spyware**

See *Configuring Antivirus/Anti-Spyware Scans for Desktops and Servers* on page 6-10

Managing the Firewall

The Firewall can block or allow certain types of network traffic by creating a barrier between the client and the network. Additionally, the Firewall will identify patterns in network packets that may indicate an attack on clients.

WFBS has two options to choose from when configuring the Firewall: simple mode and advanced mode. Simple mode enables the firewall with the Trend Micro recommended default settings. Use advanced mode to customize the Firewall settings.

Tip: Trend Micro recommends uninstalling other software-based firewalls before deploying and enabling the Trend Micro Firewall.

Default Firewall Simple Mode Settings

The Firewall provides default settings to give you a basis for initiating your client firewall protection strategy. The defaults are meant to include common conditions that may exist on clients, such as the need to access the Internet and download or upload files using FTP.

Note: By default, WFBS disables the Firewall on all new Groups and clients.

TABLE 6-2. Default Firewall Settings

SECURITY LEVEL	DESCRIPTION
Low	Inbound and outbound traffic allowed, only network viruses blocked.

SETTINGS	STATUS
Intrusion Detection System	Disabled
Alert Message (send)	Disabled

EXCEPTION NAME	ACTION	DIRECTION	PROTOCOL	PORT
DNS	Allow	Incoming and outgoing	TCP/UDP	53
NetBIOS	Allow	Incoming and outgoing	TCP/UDP	137, 138, 139, 445
HTTPS	Allow	Incoming and outgoing	TCP	443
HTTP	Allow	Incoming and outgoing	TCP	80
Telnet	Allow	Incoming and outgoing	TCP	23
SMTP	Allow	Incoming and outgoing	TCP	25
FTP	Allow	Incoming and outgoing	TCP	21
POP3	Allow	Incoming and outgoing	TCP	110
MSA	Allow	Incoming and outgoing	TCP	16372, 16373

LOCATION	FIREWALL SETTINGS
In Office	Off
Out of Office	Off

Traffic Filtering

The Firewall monitors all incoming and outgoing traffic; providing the ability to block certain types of traffic based on the following criteria:

- Direction (incoming or outgoing)
- Protocol (TCP/UDP/ICMP)
- Destination ports
- Destination computer

Scanning for Network Viruses

The Firewall examines each data packet to determine if it is infected with a network virus.

Stateful Inspection

The Firewall is a stateful inspection firewall; it monitors all connections to the client making sure the transactions are valid. It can identify specific conditions in a transaction, predict what transaction should follow, and detect when normal conditions are violated. Filtering decisions, therefore, are based not only on profiles and policies, but also on the context established by analyzing connections and filtering packets that have already passed through the firewall.

Common Firewall Driver

The Common Firewall Driver, in conjunction with the user-defined settings of the Firewall, blocks ports during an outbreak. The Common Firewall Driver also uses the Network Virus Pattern file to detect network viruses.

Configuring the Firewall

Note: Configure the Firewall for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. See *Location Awareness* on page 11-7.

Navigation Path: Security Settings > {group} > Configure > Firewall > In Office/Out of Office

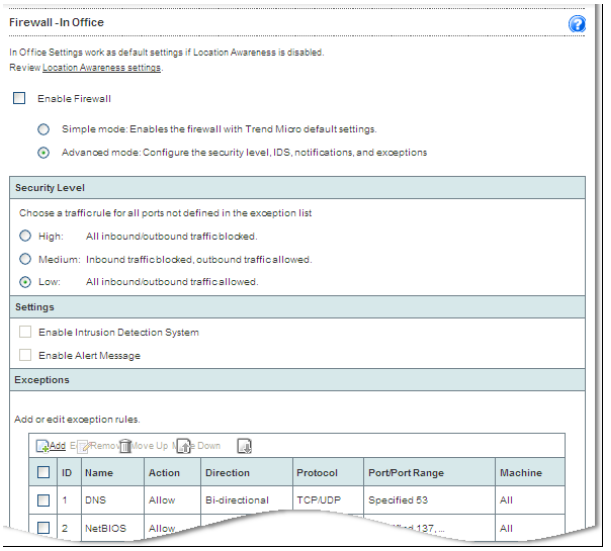


FIGURE 6-1. Firewall - In Office screen

Trend Micro default setting

- Firewall disabled

To configure the Firewall:

1. From the **Firewall** screen, update the following options as required:
   - **Enable Firewall:** Select to enable the firewall for the group and location.
     - **Simple Mode:** Enables firewall with default settings. See *Default Firewall Settings* on page 6-5.
     - **Advanced Mode:** Enables firewall with custom settings. See *Advanced Firewall Options* on page 6-8 for configuration options.
2. Click **Save.** The changes take effect immediately.

Advanced Firewall Options

Use the Advanced Firewall options to configure custom firewall settings for a particular group of clients.

To configure advanced firewall options:

1. From the **Firewall** screen, select **Advanced Mode**.
2. Update the following options as required:
   - **Security Level:** The security level controls the traffic rules to be enforced for ports not in the exception list.
     - **High:** blocks all incoming and outgoing traffic except any traffic allowed in the exception list.
     - **Medium:** blocks all incoming traffic and allows all outgoing traffic except any traffic allowed and blocked in the exception list.
     - **Low:** allows all incoming and outgoing traffic except any traffic blocked in the exception list. This is the default setting for the Simple mode.
   - Settings
     - **Enable Intrusion Detection System:** Intrusion Detection System identifies patterns in network packets that may indicate an attack. See *Intrusion Detection System* on page 6-11.
     - **Enable Alert Messages:** When WFBS detects a violation, the client is notified.
   - **Exceptions:** Ports in the exception list will not be blocked. See *Working with Firewall Exceptions* on page 6-9.
3. Click **Save**.

Working with Firewall Exceptions

The Firewall exception list contains entries you can configure to allow or block different kinds of network traffic based on Client port numbers and IP address(es). During an Outbreak, the Security Server applies the exceptions to the Trend Micro policies that are automatically deployed to protect your network.

For example, during an outbreak, you may choose to block all client traffic, including the HTTP port (port **80**). However, if you still want to grant the blocked clients access to the Internet, you can add the Web proxy server to the exception list.

Adding/Editing Exceptions

Navigation Path: Security Settings > {Group} **> Configure > Firewall > In Office or Out of Office > Advanced Mode > Exceptions > Add or** {checkbox} **Edit**

To add an Exception:

1. From the Firewall Configuration screen, click **Add**
2. See 3 below

To edit an Exception:

1. From the Firewall Configuration screen, select the Exceptions that you want to modify.
2. Click **Edit**. The Edit Exception screen opens.
3. Change the name for the exception.
4. Next to **Action**, click one of the following:
   - Allow all network traffic
   - Deny all network traffic
5. Next to Direction, click Inbound or Outbound to select the type of traffic to which to apply the exception settings.

6. Select the type of network protocol from the Protocol list:
   - **All**
   - **TCP/UDP** (default)
   - **TCP**
   - **UDP**
   - **ICMP**
7. Click one of the following to specify Client ports:
   - **All ports** (default)
   - **Range:** type a range of ports
   - **Specified ports:** specify individual ports. Use a comma "," to separate port numbers.
8. Under **Machines**, select Client IP addresses to include in the exception. For example, if you select **Deny all network traffic** (**Inbound** and **Outbound**) and type the IP address for single computer on the network, then any Client that has this exception in its policy will not be able to send or receive data to or from that IP address. Click one of the following:
   - **All IP addresses** (default)
   - **Single IP:** type the host name or IP address of a Client. To resolve the Client host name to an IP address, click Resolve.
   - **IP range:** type a range of IP addresses.
9. Click **Save.**

Editing Exceptions

Navigation Path: Security Settings > {Group} **> Configure > Firewall > In Office or Out of Office > Advanced Mode > Exceptions >** {checkbox} **> Edit**

To edit an exception:

1. From the **Firewall - Advanced Mode** screen in the **Exceptions** section, select the exclusion you want to edit.
2. Click **Edit.**

3. Update the options as required. See *Adding/Editing Exceptions* on page 6-9.
4. Click **Save.**

Removing Exceptions

To remove an exception:

1. From the **Firewall - Advanced Mode** screen, in the **Exceptions** section, select the exclusion you want to delete.
2. Click **Remove**.

Disabling the Firewall

Navigation Path: Security Settings > {group} **> Configure > Firewall > In Office/Out of Office**

To disable the Firewall:

1. To disable the firewall for the group and connection type, clear the **Enable Firewall** check box.
2. Click **Save**.

Note: To disable the Firewall on all clients, go to **Preferences > Global Settings > Desktop/Server** and select **Disable Firewall and uninstall drivers** under Firewall Settings. Disabling the Firewall will also uninstall the Firewall driver.

Intrusion Detection System

Navigation Path: Security Settings > {Group} **> Configure > Firewall > In Office or Out of Office > Advanced Mode > Settings**

Firewall also includes an Intrusion Detection System (IDS). The IDS can help identify patterns in network packets that may indicate an attack on the client. Firewall can help prevent the following well-known intrusions:

- **Oversized Fragment:** This exploit contains extremely large fragments in the IP datagram. Some operating systems do not properly handle large fragments and may throw exceptions or behave in other undesirable ways.

- **Ping of Death:** A ping of death (abbreviated **"**POD**"**) is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer.
- **Conflicting ARP:** This occurs when the source and the destination IP address are identical.
- **SYN flood:** A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of `SYN` requests to a target's system.
- **Overlapping Fragment:** This exploit contains two fragments within the same IP datagram and have offsets that indicate they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle overlapping fragments and may throw exceptions or behave in other undesirable ways. This is the basis for the so called teardrop Denial of service Attacks.
- **Teardrop Attack:** The Teardrop attack involves sending IP fragments with overlapping, over-sized, payloads to the target machine. A bug in the TCP/IP fragmentation re-assembly code of various operating systems caused the fragments to be improperly handled, crashing them as a result of this.
- **Tiny Fragment Attack:** When any fragment other than the final fragment is less than 400 bytes, indicating that the fragment is likely intentionally crafted. Small fragments may be used in denial of service attacks or in an attempt to bypass security measures or detection.
- **Fragmented IGMP:** When a client receives a fragmented Internet Group Management Protocol (IGMP) packet, the client's performance may degrade or the computer may stop responding (hang) and require a reboot to restore functionality.
- **LAND Attack:** A LAND attack is a DoS (Denial of Service) attack that consists of sending a special poison spoofed packet to a computer, causing it to behave undesirably. The attack involves sending a spoofed `TCP SYN` packet (connection initiation) with the target host's IP address and an open port as both source and destination.

Stateful Inspection

The Firewall is a stateful inspection firewall; it monitors all connections to the client making sure the transactions are valid. It can identify specific conditions in a transaction, predict what transaction should follow, and detect when normal conditions are violated. Filtering decisions, therefore, are based not only on profiles and policies, but also on the context established by analyzing connections and filtering packets that have already passed through the Firewall.

Web Reputation

Navigation Path: Security Settings > {Group} **> Configure > Web Reputation > In Office/Out of Office**

or, for Advanced:

Navigation Path: Security Settings > {MSA} Configure > Web Reputation

Web Reputation helps prevent access to URLs on the Web or embedded in email messages (Advanced only) that pose security risks by checking the URL against the Trend Micro Web Security database. Depending on the location (In Office/Out of Office) of the client (Standard Only), configure a different level of security.

Depending on the security level that has been set, it can block access to websites that are known or suspected to be a Web threat or unrated on the reputation database. Web Reputation provides both email notification to the administrator and inline notification to the user for detections.

If Web Reputation blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list. See *URL Filtering* on page 11-9.

Reputation Score

A URL's "reputation score" determines whether it is a Web threat or not. Trend Micro calculates the score using proprietary metrics.

- Trend Micro considers a URL "a Web threat", "very likely to be a Web threat", or "likely to be a Web threat" if its score falls within the range set for one of these categories.
- Trend Micro considers a URL safe to access if its score exceeds a defined threshold.

There are three security levels that determine whether the SA will allow or block access to a URL.

- **High:** Blocks pages that are:
  - **Dangerous**:Verified to be fraudulent or known sources of threats
  - **Highly suspicious:** Suspected to be fraudulent or possible sources of threats
  - **Suspicious:** Associated with spam or possibly compromised
- **Medium:** Blocks pages that are:
  - **Dangerous**:Verified to be fraudulent or known sources of threats
  - **Highly suspicious:** Suspected to be fraudulent or possible sources of threats
- **Low:** Blocks pages that are:
  - **Dangerous**:Verified to be fraudulent or known sources of threats

Configuring Web Reputation

Navigation Path: Security Settings > {group} > Configure > Web Reputation > In Office/Out of Office

or, for Advanced:

Navigation Path: Security Settings > {MSA} Configure > Web Reputation

Web Reputation evaluates the potential security risk of all requested URLs by querying the Trend Micro Security database at the time of each HTTP request.

Note: (Standard Only) Configure the Web Reputation settings for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. See *Location Awareness* on page 11-7.

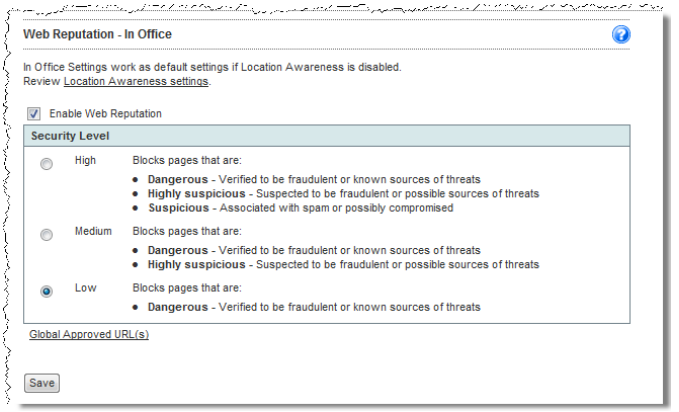


FIGURE 6-2. Web Reputation screen

To edit Web Reputation settings:

1. From the **Web Reputation** screen, update the following as required:
   - **Enable Web Reputation**
   - **Security Level**
     - **High:** Blocks pages that are:
       - **Dangerous**:Verified to be fraudulent or known sources of threats
       - **Highly suspicious:** Suspected to be fraudulent or possible sources of threats
       - **Suspicious:** Associated with spam or possibly compromised
     - **Medium:** Blocks pages that are:
       - **Dangerous**:Verified to be fraudulent or known sources of threats
       - **Highly suspicious:** Suspected to be fraudulent or possible sources of threats
     - **Low:** Blocks pages that are:
       - **Dangerous**: Verified to be fraudulent or known sources of threats
2. To modify the list of approved websites, click **Global Approved URL(s)** and modify your settings on the Global Settings screen.
3. Click **Save**.

URL Filtering

Navigation Path: Security Settings > {Group} > Configure > URL Filtering

URL Filtering blocks unwanted content from the Internet. You can select specific types of websites to block during different times of the day by selecting Custom.

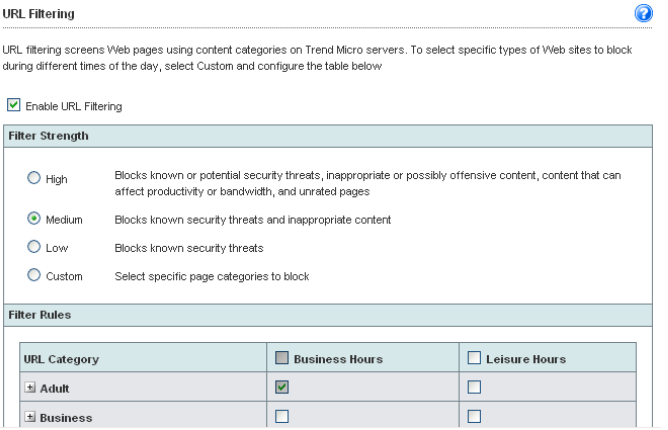


FIGURE 6-3. URL Filtering screen

From the URL Filtering screen, update the following as required:

1. **Enable URL Filtering**
2. **Filter Strength:**
   - **High:** Blocks known or potential security threats, inappropriate or possibly offensive content, content that can affect productivity or bandwidth, and unrated pages
   - **Medium:** Blocks known security threats and inappropriate content
   - **Low:** Blocks known security threats
   - **Custom:** Select your own categories, and whether you want to block the categories during business hours or leisure hours.

3. **Filter Rules:** Select entire categories or sub-categories to block.

> **Note:** To modify the list of globally approved URLs, click **Global Approved URLs** at the bottom of the screen.

4. **Business Hours**: Any days or hours that are not defined under Business Hours are considered Leisure hours.
5. **Global Approved URL(s):** Clicking this link will take you to the **Preferences > Global Settings** screen (see *Desktop/Server Options* on page 11-6).
6. Click **Save**.

Behavior Monitoring

Agents constantly monitor clients for unusual modifications to the operating system or on installed software. Administrators (or users) can create exception lists that allow certain programs to start while violating a monitored change, or completely block certain programs. In addition, programs with a valid digital signature are always allowed to start.

Another feature of Behavior Monitoring is to protect `EXE` and `DLL` files from being deleted or modified. Users with this privilege can protect specific folders. In addition, users can select to collectively protect all Intuit QuickBooks programs.

Navigation Path: Security Settings > {group} > Configure > Behavior Monitoring

Behavior Monitoring protects clients from unauthorized changes to the operating system, registry entries, other software, files and folders.

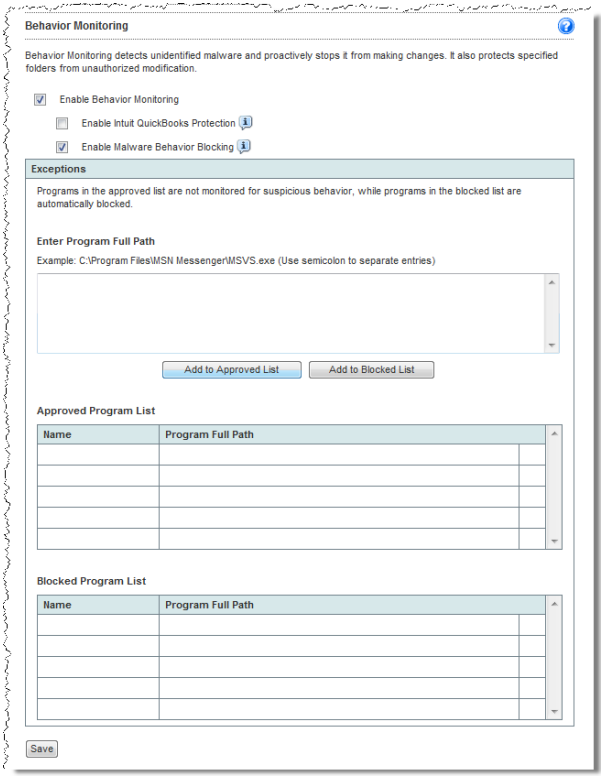


FIGURE 6-4. Behavior Monitoring screen

To edit Behavior Monitoring settings:

1. From the **Behavior Monitoring** screen, update the following as required:
   - **Enable Behavior Monitoring**

> **Note:** To allows users to customize their own Behavior Monitoring settings, go to **Security Settings >** {group} **> Configure > Client Privileges** > **Behavior Monitoring** and select **Allow users to modify Behavior Monitoring settings**.

- **Enable Intuit™ QuickBooks™ Protection:** Protects all Intuit QuickBooks files and folders from unauthorized changes by other programs. Enabling this feature will not affect changes made from within Intuit QuickBooks programs, but will only prevent changes to the files from other unauthorized applications.

  The following products are supported:

  QuickBooks Simple Start

  QuickBooks Pro

  QuickBooks Premier

  QuickBooks Online

- **Enable Malware Behavior Blocking:** A group of technologies based on rule sets that attempt to identify certain suspicious behaviors that are common amongst malware or Fake Anti-Virus. Examples of such behaviors may include sudden and unexplainable new running services, changes to the firewall, system file modifications, etc.
- **Exceptions:** Exceptions include an **Approved Program List** and a **Blocked Program List**: Programs in the **Approved Programs List** can be started even if it violates a monitored change, while programs in the **Blocked Program List** can never be started.
  - **Enter Program Full Path:** Type the full Windows or UNC path of the program. Separate multiple entries with semicolons. Click **Add to Approved List** or **Add to Blocked List**. Use environment variables to specify paths, if required. See *Table 6-3* on page 6-20 for the list of supported variables.
  - **Approved Program List:** Programs (maximum of 100) in this list can be started. Click the corresponding  icon to delete an entry.
  - **Blocked Program List:** Programs (maximum of 100) in this list can never be started. Click the corresponding  icon to delete an entry.

2. Click **Save**.

Environment Variables

WFBS supports environment variables to specify specific folders on the client. Use these variables to create exceptions for specific folders. The following table describes the available variables:

TABLE 6-3. Supported Variables

ENVIRONMENT VARIABLE	POINTS TO THE...
$windir$	Windows folder
$rootdir$	root folder
$tempdir$	Windows temporary folder
$programdir$	Program Files folder

Device Control

Navigation Path: Security Settings > {group} > Configure > Device Control

Device Control regulates access to external storage devices and network resources connected to computers.

Set the following as required:

- **Enable Device Control**
- **Enable USB Autorun Prevention**
- **Permissions:** set for both USB devices and network resources. For both, set:

TABLE 6-4. Device Control Permissions

PERMISSIONS	
Full access	Operations allowed: Copy, Move, Open, Save, Delete, Execute
No access	Any attempt to access the device or network resource is automatically blocked.
Read only	Operations allowed: Copy, Open Operations blocked: Save, Move, Delete, Execute
Read and write only	Operations allowed: Copy, Move, Open, Save, Delete Operation blocked: Execute
Read and execute only	Operations allowed: Copy, Open, Execute Operations blocked: Save, Move, Delete

- **Exceptions:** If a user is not given read permission for a particular device, the user will still be allowed to run or open any file or program in the Approved List.

  However, if AutoRun prevention is enabled, even if a file is included in the Approved List, it will still not be allowed to run.

  To add an exception to the Approved List, enter the file name including the path or the digital signature and click **Add to the Approved List**

User Tools

User Tools comprises a set of client tools that enable users to surf the Web securely:

- **Wi-Fi Advisor:** Determines the safety of a wireless connection by checking the authenticity of access points based on the validity of their SSIDs, authentication methods, and encryption requirements. A pop-up warning will show if a connection is unsafe.
- **Trend Micro Toolbar:** Uses Page Ratings to determine the safety of web pages. Warns users about malicious and Phishing websites. Ratings will appear in Google/Yahoo/Bing search results.
- **Anti-Spam Toolbar:** Filters spam in Microsoft Outlook, gives statistics, and allows you to change certain settings.

Anti-Spam Toolbar Requirements

The Trend Micro Anti-Spam toolbar supports the following mail clients:

- Microsoft Outlook 2003, 2007, 2010
- Outlook Express 6.0 with Service Pack 2 (on Windows XP only)
- Windows Mail (on Windows Vista only)

The Anti-Spam toolbar supports the following operating systems:

- Windows XP SP2 32-bit
- Windows Vista 32- and 64-bit
- Windows 7 32- and 64-bit

Configuring User Tools

Navigation Path: Security Settings > {desktop group} **> Configure > User Tools**

To edit the availability of User tools:

1. From the **User Tools** screen, update the following as required:
   - **Enable Wi-Fi Advisor:** Checks the safety of wireless networks based on the validity of their SSIDs, authentication methods, and encryption requirements.

- **Enable Page Ratings:** Determines the safety of the current page.
- **Enable anti-spam toolbar in supported mail clients**

2. Click **Save.**

Note: Toolbars can only be made available to Agents from the Web Console. Users have to install or uninstall the tools from the Agent's console.

Configuring Client Privileges

Navigation Path: Security Settings > {group} > Configure > Client Privileges

Grant Client Privileges to allow users to modify settings of the Agent installed on their computer.

Tip: To enforce a regulated security policy throughout your organization, Trend Micro recommends granting limited privileges to users. This ensures users do not modify scan settings or unload the Security Agent.

Configuring Client Privileges

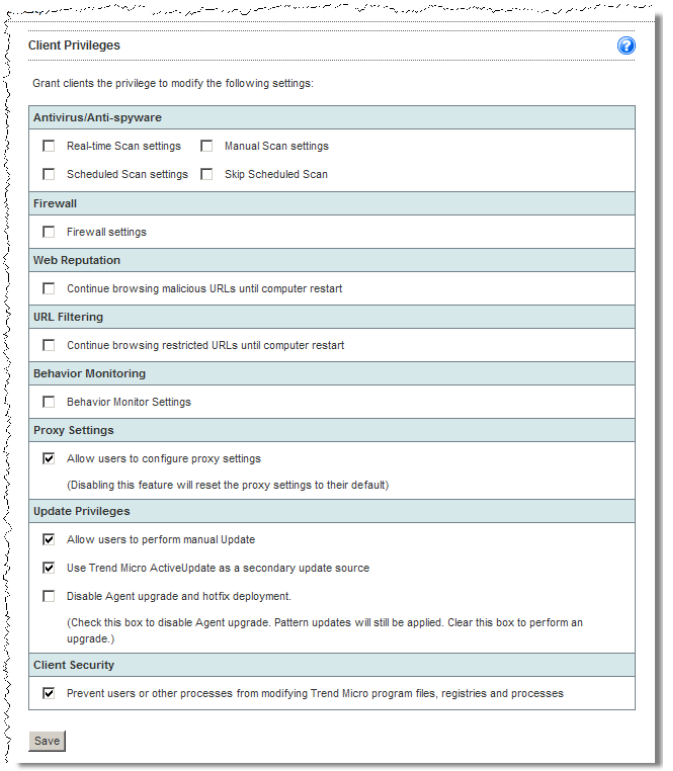


FIGURE 6-5. Client Privileges screen

To grant privileges to Clients:

1. From the **Client Privileges** screen, update the following as required:
   - **Antivirus/Anti-spyware**
     - **Manual Scan settings**
     - **Scheduled Scan settings**
     - **Real-time Scan settings**
     - **Skip Scheduled Scan**

- **Firewall**
  - Firewall Settings
- **Web Reputation**
  - Will show a link that allows users to continue browsing a particular malicious URL until the computer is restarted. Warnings will still show on other malicious URLs.
- **URL Filtering**
  - Will show a link that allows users to continue browsing a particular restricted URL until the computer is restarted. Warnings will still show on other restricted URLs.
- **Behavior Monitoring**
  - Allow users to modify Behavior Monitor settings.
- **Proxy Setting**s
  - **Allow users to configure proxy settings.** Disabling this feature will reset the proxy settings to their default.
- **Update Privileges**
  - **Allow users to perform manual Update**
  - **Use Trend Micro ActiveUpdate as a secondary update source**
- **Client Security**
  - **Prevent users or other processes from modifying Trend Micro program files, registries and processes.**

2. Click **Save**.

Configuring the Quarantine

The quarantine directory stores infected files. The quarantine directory can reside on the client itself or on another server (Also see *Messaging Agent Quarantine* on page 9-93 (Advanced only)). If an invalid quarantine directory is specified, Agents use the default quarantine directory on the client.

The default folder on the client is:

```
C:\Program Files\Trend Micro\AMSP\quarantine
```

The default folder on the server is:

```
C:\Program Files\Trend Micro\Security Server\PCCSRV\Virus
```

Note: If the SA is unable to send the file to the Security Server for any reason, such as a network connection problem, the file remains in the client suspect folder. The Agent attempts to resend the file when it reconnects to the Security Server.

Configuring the Quarantine Directory

Navigation Path: Security Settings > {group} > Configure > Quarantine

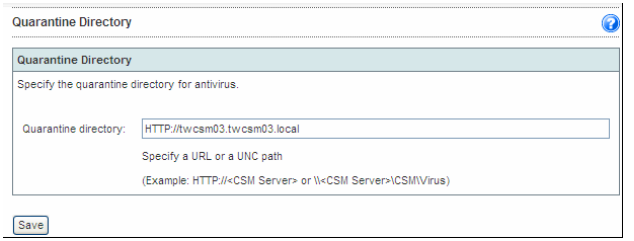


FIGURE 6-6. Quarantine Directory screen

To set the Quarantine directory:

1. From the Quarantine Directory screen, update the following as required:
   - **Quarantine directory:** Type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path to store the infected files. For example, `http://www.example.com/quarantine` or `\\TempServer\Quarantine`.
2. Click **Save**.

Appendix A

Troubleshooting and Frequently Asked Questions

This appendix provides solutions to common problems and answers common questions.

The topics discussed in this appendix include:

Troubleshooting

This section helps you troubleshoot issues that may arise while installing or using WFBS.

Environments with Restricted Connections

If your environment has restrictions connecting to the Internet, in the case of a closed LAN or lack of an Internet connection, use the following procedures:

If Agents can access the Security Server:

1. Create a new package using the Client Packager (*Installing with Client Packager* on page 3-9).
2. Manually install the package on the computer.

The Agent now applies the security settings as configured on the server.

If Agents cannot access the Security Server:

1. Create a new package using the Client Packager.
2. Manually install the package on the computer.

Client Packager Post-Installation Problems

If you installed the Agent with Client Packager and are encountering problems, consider the following:

- **Install:** If the Agent cannot connect to the Security Server, the client will keep default settings. Only when the client can connect to the Security Server can it obtain group settings.
- **Upgrade:** If you encounter problems upgrading the Agent with Client Packager, Trend Micro recommends uninstalling the previous version of the Agent first, then installing the new version.

User's Spam Folder not Created (Advanced only)

When the Administrator creates a mailbox account for a user, the spam folder is not created immediately in Microsoft Exchange server, but will be created under the following conditions:

- An end user logs on to their mailbox for the first time
- The first email arrives at the mailbox

The Administrator must first create the mailbox entity and the user must log on before EUQ can create a spam folder.

Internal Sender-Recipient Confusion (Advanced only)

You can only define one domain as the internal address for the Messaging Security Agent. If you use Microsoft Exchange System Manager to change your primary address on a server, Messaging Security Agent does not recognize the new address as an internal address because Messaging Security Agent cannot detect that the recipient policy has changed.

For example, you have two domain addresses for your company: @example_1.com and @example2.com. You set @example_1.com as the primary address. Messaging Security Agent considers email messages with the primary address to be internal (that is, abc@example_1.com, or xyz@example_1.com are internal). Later, you use Microsoft Exchange System Manager to change the primary address to @example_2.com. This means that Microsoft Exchange now recognizes addresses such as abc@example_2.com and xyz@example_2.com to be internal addresses.

Re-sending a Quarantine Message Fails (Advanced only)

This can happen when the system administrator's account on the Microsoft Exchange server does not exist.

To resolve quarantined message failure:

1. Using the Windows Registry Editor, open the following registry entry on the server:
   `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

2. Edit the entry as follows:

WARNING! **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- `ResendMailbox` {Administrator Mailbox} (for example, admin@example.com)
- `ResendMailboxDomain` {Administrator's Domain} (for example, example.com)
- `ResendMailSender` {Administrator's Email Account} (for example, admin

3. Close the Registry Editor.

MSA SQL Server Dependency in Exchange Server 2007 (Advanced only)

In computers running Exchange Server 2007, the Messaging Security Agent (MSA) uses a SQL Server database. To prevent issues, MSA services are designed to be dependent on the SQL Server service instance **MSSQL$SCANMAIL**. Whenever this instance is stopped or restarted, the following MSA services are also stopped:

- ScanMail_Master
- ScanMail_RemoteConfig

Manually restart these MSA services if **MSSQL$SCANMAIL** is stopped or restarted. Different events, including when SQL Server is updated, can cause **MSSQL$SCANMAIL** to restart or stop.

Saving and Restoring Program Settings

You can save a copy of the WFBS database and important configuration files for rolling back your WFBS program. You may want to do this if you are experiencing problems and want to reinstall WFBS or if you want to revert to a previous configuration.

To restore program settings after rollback or reinstallation:

1. Stop the Trend Micro Security Server Master Service.

2. Manually copy the following files and folders from the folder to an alternate location:

   WARNING! Do not use backup tools or applications for this task.

   `C:\Program Files\Trend Micro\Security Server\PCCSRV`

   - **`ofcscan.ini`:** Contains global settings.
   - **`ous.ini`:** Contains the update source table for antivirus component deployment.
   - **`Private` folder:** Contains firewall and update source settings.
   - **`Web\TmOPP` folder:** Contains Outbreak Defense settings.
   - **`Pccnt\Common\OfcPfw.dat`:** Contains firewall settings.
   - **`Download\OfcPfw.dat`:** Contains firewall deployment settings.
   - **`Log` folder:** Contains system events and the verify connection log.
   - **`Virus` folder:** The folder in which WFBS quarantines infected files.
   - **`HTTDB` folder:** Contains the WFBS database.

3. Uninstall WFBS.
4. Perform a fresh install. See the WFBS *Installation Guide*.
5. After the master installer finishes, stop the Trend Micro Security Server Master Service on the target computer.

6. Update the virus pattern version from the backup file:

   a. Get current virus pattern version from the new server.

   ```
   \Trend Micro\Security Server\PCCSRV\Private\component.ini.
   [6101]

   ComponentName=Virus pattern

   Version=xxxxxx 0 0
   ```

   b. Update the version of the virus pattern in the backed-up file:

   ```
   \Private\component.ini
   ```

   Note: If you change the Security Server installation path, you will have to update the path info in the backup files `ofcscan.ini` and `\private\ofcserver.ini`

7. With the backups you created, overwrite the WFBS database and the relevant files and folders on the target machine in the `PCCSRV` folder.
8. Restart the Trend Micro Security Server Master Service.

Some Components are not Installed

Licenses to various components of Trend Micro products may differ by region. After installation, you will see a summary of the components your Registration Key/Activation Code allows you to use. Check with your vendor or reseller to verify the components for which you have licenses.

Unable to Access the Web Console

This section discusses the possible causes for being unable to access the Web Console.

Browser Cache

If you upgraded from a previous version of WFBS, Web browser and proxy server cache files may prevent the Web Console from loading. Clear the cache memory on your browser and on any proxy servers located between the Trend Micro Security Server and the computer you use to access the Web Console.

SSL Certificate

Also, verify that your Web server is functioning properly. If you are using SSL, verify that the SSL certificate is still valid. See your Web server documentation for details.

Virtual Directory Settings

There may be a problem with the virtual directory settings if you are running the Web Console on an IIS server and the following message appears:

The page cannot be displayed
HTTP Error 403.1 - Forbidden: Execute access is denied.
Internet Information Services (IIS)

This message may appear when either of the following addresses is used to access the console:

```
http://{server name}/SMB/
```

```
http://{server name}/SMB/default.htm
```

However, the console may open without any problems when using the following address:

```
http://{server name}/SMB/console/html/cgi/cgichkmasterpwd.exe
```

To resolve this issue, check the execute permissions of the SMB virtual directory.

To enable scripts:

1. Open the Internet Information Services (IIS) manager.
2. In the SMB virtual directory, select **Properties**.
3. Select the **Virtual Directory** tab and change the execute permissions to **Scripts** instead of none. Also, change the execute permissions of the client install virtual directory.

Incorrect Number of Clients on the Web Console

You may see that the number of clients reflected on the Web Console is incorrect.

This happens if you retain client records in the database after removing the Agent. For example, if client-server communication is lost while removing the Agent, the server does not receive notification about the Agent removal. The server retains client information in the database and still shows the client icon on the console. When you reinstall the Agent, the server creates a new record in the database and displays a new icon on the console.

Use the Verify Connection feature through the Web Console to check for duplicate client records.

Client Icon Does Not Appear on Web Console After Installation

You may discover that the client icon does not appear on the Web Console after you install the Agent. This happens when the client is unable to send its status to the server.

To check communication between Clients and the Web Console:

- Open a Web browser on the Client, type

  ```
  https://{Trend Micro Security Server_Name}:
  {port number}/SMB/cgi/cgionstart.exe
  ```

  in the address text box, and then press **ENTER**. If the next screen shows **-2**, this means the Client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record of the Client.
- Verify that client-server communication exists by using ping and telnet.
- If you have limited bandwidth, check if it causes connection timeout between the server and the client.
- Check if the `\PCCSRV` folder on the server has shared privileges and if all users have been granted full control privileges
- Verify that the Trend Micro Security Server proxy settings are correct.

Issues During Migration from Other Antivirus Software

This section discusses some issues you may encounter when migrating from third-party antivirus software.

The setup program for the Security Agent uses the third-party software's uninstallation program to automatically remove it from your users' system and replace it with the Security Agent. If automatic uninstallation is unsuccessful, users get the following message:

```
Uninstallation failed.
```

There are several possible causes for this error:

- The third-party software's version number or product key is inconsistent.
- The third-party software's uninstallation program is not working.
- Certain files for the third-party software are either missing or corrupted.
- The registry key for the third-party software cannot be cleaned.
- The third-party software has no uninstallation program.

There are also several possible solutions for this error:

- Manually remove the third-party software.
- Stop the service for the third-party software.
- Unload the service or process for the third-party software.

Unsuccessful Web Page or Remote Installation

If users report that they cannot install from the internal Web page or if installation with Remote install is unsuccessful, try the following methods.

- Verify that client-server communication exists by using ping and telnet.
- Check if TCP/IP on the client is enabled and properly configured.
- If you are using a proxy server for client-server communication, check of the proxy settings are configured correctly.
- In the Web browser, delete Trend Micro add-ons and the browsing history.

Unable to Replicate Messaging Security Agent Settings (Advanced only)

You can only replicate settings from a source Messaging Security Agent to a target Messaging Security Agent that share the same domain.

For Windows 2003, do the first 4 steps:

1. Start **regedit**.
2. Go to

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
   ```

3. Right click **winreg > Permissions**.
4. Add **Smex Admin Group** of target domain, and enable **Allow Read**.

Frequently Asked Questions (FAQs)

The following is a list of frequently asked questions and answers.

Where Can I Find My Activation Code and Registration Key?

You can activate WFBS during the installation process or later using the Web Console. To activate WFBS, you need to have an Activation Code.

Obtaining an Activation Code

You automatically get an evaluation Activation Code if you download Worry-Free Business Security from the Trend Micro website.

You can use a Registration Key to obtain an Activation Code online.

Activation Codes have 37 characters and look like this:

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

Obtaining a Registration Key

The Registration Key can be found on:

- Product CD
- License Certificate (which you obtained after purchasing the product)

Registering and activating your copy of WFBS entitles you the following benefits:

- Updates to the WFBS pattern files and scan engine
- Technical support
- Easy access in viewing the license expiration update, registration and license information, and renewal reminders
- Easy access in renewing your license and updating the customers profile

Registration Keys have 22 characters and look like this:

```
xx-xxxx-xxxx-xxxx-xxxx
```

When the full version expires, security updates will be disabled; when the evaluation period expires, both the security updates and scanning capabilities will be disabled. In the Product License screen, you can obtain an Activation Code online, view renewal instructions, and check the status of your product.

Registration

I have several questions on registering WFBS. Where can I find the answers?

See the following website for frequently asked questions about registration:

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

Installation, Upgrade, and Compatibility

Which versions of Worry-Free Business Security or Worry-Free Business Security Advanced can upgrade to this version?

See the WFBS *Installation Guide* for information.

Which Agent installation method is best for my network environment?

See the *Installing Security Agents to Desktops and Servers* on page 3-2 for a summary and brief comparison of the various Agent installation methods available.

Can the Trend Micro Security Server be installed remotely using Citrix or Windows Terminal Services?

Yes. The Trend Micro Security Server can be installed remotely with Citrix or Windows Terminal Services.

Does WFBS support 64-bit platforms?

Yes. A scaled down version of the Security Agent is available for the x64 platform. However, no support is currently available for the IA-64 platform.

Can I upgrade to WFBS from Trend Micro™ ServerProtect?

No. ServerProtect will have to be first uninstalled and then WFBS can be installed.

Can I use a pre-existing installation of an Apache Web server on computer where I am installing the Security Server?

Trend Micro recommends that you do not use a pre-existing installation of Apache. The correct version will be installed at the same time that you install the Security Server.

How Can I Recover a Lost or Forgotten Password?

Access to the Worry-Free Business Security console requires a password which is first defined during installation and can be subsequently changed at any time. If you have forgotten your password, you can use the Console Password Reset Tool to reset the password. Access this tool on the Security Server computer under the Trend Micro Worry-Free Business Security folder in the Windows Start menu.

Intuit Software Protection

What happens when an attempted Intuit update is blocked?

All Intuit executable files have a digital signature and updates to these files will not be blocked. If there are other programs try to change the Intuit binary file, the Agent displays a message with the name of the program that is attempting to update the binary files.

Can other programs be allowed to update Intuit files? Can I bypass Trend Micro protection on a case-to-case basis?

Yes. To allow this, add the required program to the Behavior Monitoring Exception List on the Agent.

WARNING! **Remember to remove the program from the exception list after the update.**

Configuring Settings

I have several questions on configuring WFBS settings. Where can I find the answers?

You can download all WFBS documentation from the following site:

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

What folders should I exclude for Antivirus software with SBS 2003?

See the following tables for the SBS 2003 exclusions:

TABLE A-1. Microsoft Exchange Exclusions (Advanced only)

Microsoft Exchange Server Database	C:\Program Files\Exchsrvr\MDBDATA
Microsoft Exchange MTA files	C:\Program Files\Exchsrvr\Mtadata
Microsoft Exchange Message tracking log files	C:\Program Files\ Exchsrvr\server_name.log
Microsoft Exchange SMTP Mailroot	C:\Program Files\Exchsrvr\Mailroot
Microsoft Exchange working files	C:\Program Files\Exchsrvr\MDBDATA
Site Replication Service	C:\Program Files\Exchsrvr\srsdata C:\Program Files\Exchsrvr\conndata

TABLE A-2. IIS Exclusions

IIS System Files	C:\WINDOWS\system32\inetsrv
IIS Compression Folder	C:\WINDOWS\IIS Temporary Compressed Files

TABLE A-3. Domain Controller Exclusions

Active Directory database files	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
NTFRS Database Files	C:\WINDOWS\ntfrs

TABLE A-4. Windows SharePoint Services Exclusions

Temporary SharePoint folder	C:\windows\temp\FrontPageTempDir

TABLE A-5. Client Desktop Folder Exclusions

Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore

TABLE A-6. Additional Exclusions

Removable Storage Database (used by SBS Backup)	C:\Windows\system32\NtmsData
SBS POP3 connector Failed Mail	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail
SBS POP3 connector Incoming Mail	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail
Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore
DHCP Database Store	C:\WINDOWS\system32\dhcp
WINS Database Store	C:\WINDOWS\system32\wins

Do I Have the Latest Pattern File or Service Pack?

The updatable files will very depending on which product you have installed.

To find out if you have the latest pattern file or service pack:

1. From the Web Console, click **Preferences > Product License**. The Product License screen appears.
2. Product license details, including the current product version appears.

To find out the latest available patterns, open a Web browser to one of the following:

- The Trend Micro Update Center:

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

- The Trend Micro Pattern File:

  http://www.trendmicro.com/download/pattern.asp

Smart Scan

What is Smart Scan?

Smart Scan is a new technology from Trend Micro that uses a central scan server on the network to take some of the burden of scanning off clients.

Is Smart Scan reliable?

Yes. Smart Scan simply allows another computer, the Smart Scan Server, to help scan your clients. If your clients are configured for Smart Scan but cannot connect to the Smart Scan Server, they will attempt to connect to the Trend Micro Global Smart Scan Server.

How do I know if the Smart Scan Server is running properly?

Verify that the following service is running on the Security Server:

```
TMiCRCScanService
```

Can I uninstall the Scan Server or choose not to install it?

No. If you do not want to use Smart Scan, disable the Smart Scan service, which switches all clients to Conventional Scan and stops the Smart Scan service on the Security Server. This can also help improve the performance of the Security Server. See *General Scan Settings* on page 11-8 for instructions.

Known Issues

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

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

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

http://esupport.trendmicro.com/support/

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

Appendix B

Getting Help

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

The topics discussed in this appendix include:

Product Documentation

The documentation for WFBS consists of the following:

- Online Help

  Web-based documentation accessible from the Web Console.

  The WFBS *Online Help* describes the product features and gives instructions on their use. It contains detailed information about customizing your settings and running security tasks. Click the icon to open context-sensitive help.

  Who should use the online help?

  WFBS Administrators who need help with a particular screen.

- Installation Guide

  The *Installation Guide* provides instructions to install/upgrade the product and get started. It provides a description of the basic features and default settings of WFBS.

  The *Installation Guide* is accessible from the Trend Micro SMB CD or can be downloaded from the Trend Micro Update Center:

  http://www.trendmicro.com/download

  Who should read this guide?

  WFBS Administrators who want to install and get started with WFBS.

- Administrator's Guide

  The *Administrator's Guide* provides a comprehensive guide for configuring and maintaining the product.

  The *Administrator's Guide* is accessible from the Trend Micro SMB CD or can be downloaded from the Trend Micro Update Center:

  http://www.trendmicro.com/download

  Who should read this guide?

  WFBS Administrators who need to customize, maintain, or use WFBS.

- Readme file

  The *Readme file* contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, license information, and so on.

- Knowledge Base

The *Knowledge Base* is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website:

http://esupport.trendmicro.com

Trend Micro is always seeking to improve its documentation. For questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. You can also evaluate this documentation on the following site:

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

Knowledge Base

The Trend Micro Knowledge Base is an online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use the Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in the Knowledge Base are product FAQs, tips, advice on preventing virus/malware infections, and regional contact information for support and sales.

The Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

http://esupport.trendmicro.com/support/smb/search.do

Technical Support

When you contact Trend Micro Technical Support, to speed up your problem resolution, run the Case Diagnostic Tool (refer *Using the Case Diagnostic Tool* on page B-4) or ensure that you have the following details available:

- Operating system
- Network type
- Brand and model of the computer and connected hardware
- Amount of memory and free hard disk space on your machine
- Detailed description of the installation environment

- Exact text of any error message
- Steps to reproduce the problem

To contact Trend Micro Technical Support:

1. Run the Case Diagnostic Tool. For more information, refer *Using the Case Diagnostic Tool* on page B-4.
   - Visit the following URL:

     http://esupport.trendmicro.com/support/srf/questionentry.do

     Click the link for the required region. Follow the instructions for contacting support in your region.
   - If you prefer to communicate by email message, send a query to the following address:

     virusresponse@trendmicro.com
   - In the United States, you can also call the following toll-free telephone number:

     `(877) TRENDAV, or 877-873-6328`

Using the Case Diagnostic Tool

Use the Case Diagnostic Tool to collect Trend Micro software settings and environment setup specifications from the computer. This information is used to troubleshoot problems related to the software.

Download the Case Diagnostic Tool from:

http://www.trendmicro.com/download/product.asp?productid=25

Contacting Trend Micro

Trend Micro has sales and corporate offices in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

http://us.trendmicro.com/us/about/contact_us

Note: The information on this website is subject to change without notice.

Trend Micro provides technical support, virus 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.

Trend Micro Incorporated provides worldwide support to all of our registered users.

Get a list of the worldwide support offices:

http://www.trendmicro.com/support

Get the latest Trend Micro product documentation:

http://www.trendmicro.com/download

In the United States, you can reach the Trend Micro representatives via 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

Email: support@trendmicro.com

Sending Suspicious Files to Trend Micro

You can send your virus/malware, infected files, Trojans, suspected worms, and other suspicious files to Trend Micro for evaluation. To do so, contact your support provider or visit the Trend Micro Submission Wizard URL:

http://subwiz.trendmicro.com/SubWiz

Click the link under the type of submission you want to make.

Note: Submissions made through the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you submit your case, an acknowledgement screen displays. This screen also displays a case number. Make note of the case number for tracking purposes.

Virus Threat Enclyclopedia

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Threat Enclyclopedia website:

http://www.trendmicro.com/vinfo/

Visit the Threat Enclyclopedia to:

- Read the Weekly Virus Report, which includes a listing of threats expected to trigger in the current week and describes the 10 most prevalent threats around the globe for the current week.
- View a Virus Map of the top 10 threats around the globe.
- Consult the Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes.
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured.
- Read general virus/malware information, such as:
  - The Virus Primer, which helps you understand the difference between virus/malware, Trojans, worms, and other threats
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
  - A glossary of virus/malware and other security threat terminology
- Download comprehensive industry white papers

- Subscribe to Trend Micro Virus Alert service to learn about outbreaks as they happen and the Weekly Virus Report
- Learn about free virus/malware update tools available to Web masters.
- Read about TrendLabs^{SM}, the Trend Micro global antivirus research and support center

TrendLabs

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

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

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support 24x7.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

Appendix C

Glossary

The Glossary provides descriptions of important terms and concepts used in this document. For information on security threats, see:

http://threatinfo.trendmicro.com/vinfo/

For information about how the Trend Micro Smart Protection Network protects you, see:

http://itw.trendmicro.com/smart-protection-network

TABLE C-1. Glossary

TERM	DESCRIPTION
Activation Code	A numerical code required to enable scanning and product updates. You can activate your product during installation or anytime thereafter. If you do not have the Activation Code(s), use the Registration Key that came with your product to register on the Trend Micro website and receive the Activation Code(s).
ActiveUpdate	Connected to the Trend Micro update website, ActiveUpdate provides updated downloads of components such as the virus pattern files, scan engines, and program files. ActiveUpdate is a function common to many Trend Micro products.
Agent	The WFBS program that runs on the client.
clean	To remove virus code from a file or message.
Cleanup	Cleanup detects and removes Trojans and applications or processes installed by Trojans. It repairs files modified by Trojans.
Clients	Clients are Microsoft Exchange servers, desktops, portable computers, and servers where a Messaging Security Agent or a Security Agent is installed.
Compressed File	A single file containing one or more separate files plus information for extraction by a suitable program, such as WinZip and 7zip.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
Content Filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.

TABLE C-1. Glossary (Continued)

TERM	DESCRIPTION
Conventional Scan	A local scan engine on the client scans the client computer.
Domain Name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
End User License Agreement (EULA)	An End User License Agreement, or EULA, is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking “I accept” during installation. Clicking “I do not accept” will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware/grayware and other types of grayware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software.
False Positive	A false positive occurs when a file is incorrectly detected by security software as infected.
HTTP	Hypertext Transfer Protocol (HTTP) is a standard protocol used for transporting web pages (including graphics and multimedia content) from a server to a client over the Internet.
HTTPS	Hypertext Transfer Protocol using Secure Socket Layer (SSL). HTTPS is a variant of HTTP used for handling secure transactions.
IP	"The internet protocol (IP) provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)

TABLE C-1. Glossary (Continued)

TERM	DESCRIPTION
JAVA	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets". An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet transfers its code to your computer and the browser's Java Virtual Machine executes the applet.
Listening Port	A listening port is utilized for client connection requests for data exchange. The default Trend Micro Security listening port is 61617. If a firewall application is running on the server computer, ensure that the firewall does not block the listening port to ensure uninterrupted communication between the server and clients.
Live Status	The main screen of the Web Console. The Live Status screen gives you an at-a-glance security status for Outbreak Defense, Antivirus, Anti-spyware, and Network Viruses.
Web Console	The Web Console is a centralized Web-based management console. You can use it to configure the settings of Security Agents and Messaging Security Agents which are protecting all your remote desktops, servers and Microsoft Exchange servers. The Web Console is installed when you install the Trend Micro Security Server and uses Internet technologies such as ActiveX, CGI, HTML, and HTTP.
Pattern Matching	Since each virus contains a unique "signature" or string of telltale characters that distinguish it from any other code, the virus experts at Trend Micro capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When the engine detects a match, a virus has been detected and an email notification is sent to the Administrator.

TABLE C-1. Glossary (Continued)

TERM	DESCRIPTION
Port Number	A port number, together with a network address - such as an IP number, allow computers to communicate across a network. Each application program has a unique port number associated with it. Blocking a port on a computer prevents an application associated with that port number from sending or receiving communications to other applications on other computers across a network. Blocking the ports on a computer is an effective way to prevent malicious software from attacking that computer.
Proxy Server	A proxy server is a World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, and then returns the URL to the requester.
privileges (client privileges)	From the Web Console, Administrators can set privileges for the Security Agents. End users can then set the Security Agents to scan their clients according to the privileges you allowed. Use client privileges to enforce a uniform antivirus policy throughout your organization.
Registration Key	A numerical code required to register with Trend Micro and obtain an Activation Code.
Scan Server	The Scan Server downloads scanning-specific components from Trend Micro and uses them to scan clients. The Scan Server is available on the same computer as the Security Server.
Security Server	When you first install WFBS, you install it on a Windows server that becomes the Security Server. The Security Server communicates with the Security Agents and the Messaging Security Agents installed on clients. The Security Server also hosts the Web Console, the centralized Web-based management console for the entire WFBS solution.
Smart Scan	A Scan Server helps scan the client.

TABLE C-1. Glossary (Continued)

TERM	DESCRIPTION
SSL	Secure Socket Layer (SSL) is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
TCP	A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP relies on IP datagrams for address resolution. See DARPA Internet Program RFC 793 for information.
Telnet	Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.
TrendLabs	TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.

TABLE C-1. Glossary (Continued)

TERM	DESCRIPTION
TrendSecure	TrendSecure comprises a set of browser-based plugin tools (Trend Micro Toolbar and the Wi-Fi Advisor) that enable users to surf the Web securely. The Trend Micro Toolbar warns users about malicious and Phishing websites. The Wi-Fi Advisor determines the safety of your wireless connection by checking the authenticity of the access point.
True File Type	Files can be easily renamed to disguise their actual type. Programs such as Microsoft Word are “extension independent” -- they will recognize and open “their” documents regardless of the file name. This poses a danger, for example, if a Word document containing a macro virus has been named “benefits form.pdf”. Word will open the file, but the file may not have been scanned if the Security Agent or the Messaging Security Agent is not set to check the true file type.
Update Agent	Agents that act as update sources for other Agents.

Index

L

M

N

O

P

Q

R

S

T

U

V

W