TREND MICRO

Worry-Free™ Business Security Advanced 6

#1 for Small Business Security

Installation Guide

Document Part Number: WBEM64408/100209

Release Date: August 2010

Product Name and Version No.: Trend Micro™ Worry-Free™ Business Security 6.0 SP3

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 Web site.

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 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

Chapter 1

Introducing Trend Micro™ Worry-Free™ Business Security Advanced

This chapter provides an overview of Trend Micro Worry-Free Business Security Advanced (WFBS) key features and capabilities.

The topics discussed in this chapter include:

Overview of Trend Micro Worry-Free Business Security Advanced

Trend Micro Worry-Free Business Security Advanced (WFBS) protects small business users and assets from data theft, identity theft, risky Web sites, and spam. Powered by the Trend Micro™ Smart Protection Network, Worry-Free Business Security Advanced is:

- **Safer:** Stops viruses, spyware, spam, and Web threats from reaching computers or servers. URL filtering blocks access to risky Web sites 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 6.0

- S**mart Scan:**

  Smart Scan moves sizable malware and spyware scanning functionality to a scan server.

  It keeps client footprints small and reduces the need for clients to constantly download updates, defending against the unprecedented rates at which threats are ow being released.

  By delivering solutions to a server instead of updating individual clients, it can provide the latest protection almost instantly.

  See *Scan Methods* on page 7-2 and *Selecting the Scan Method* on page 7-3 for more information.

- **URL Web Content Filtering**:

  Rely on Trend Micro to block Web sites that contain inappropriate content. URL filtering can help improve employee productivity, secure network resources, and protect proprietary information.

  See *Configuring URL Filtering* on page 6-18 for more information.

- **Smart Protection Network Integration:**

  The Trend Micro Smart Protection Network is a collection of technologies that gathers a wide variety of threat-related information from across the Internet to provide up-to-date protection from the latest threats.

  URL Filtering, Web Reputation, and Smart Scan are all integral parts of the Trend Micro Smart Protection Network.

  See *Participating in the Smart Protection Network* on page 12-5 for more information.

- **Simpler and Easier Live Status:**

  The Live Status dashboard is now even easier to read.

  See *Live Status* on page 5-5 for more information.

- **Integrated Installation with Worry-Free™ Remote Manager 2.1**:

  Resellers now have the option to install a Worry-Free Remote Manager Agent that will allow the resellers to remotely manage a newly installed WFBS Security Server.

  See *Installing the Trend Micro™ Worry-Free™ Remote Manager Agent* on page 3-35 for more information.

- **New Graphical Interface for Restore Encrypted Virus Quarantine Tool:**

  Provides easier quarantine management when using the Restore Encrypted Virus tool.

  See *Restore Encrypted Virus* on page E-10 for more information.

- **Variable Scanning Based on CPU Usage:**

  Provides added flexibility for scanning when the CPU usage is high. WFBS is now CPU-sensitive and can be configured to pause during high CPU consumption.

  See *Configuring Manual and Scheduled Scan Options* on page 7-3 for more information.

- **Protection from USB Autorun Threats:**

  Prevents autorun files on USB drives from executing when the drive is inserted in the USB port of a client.

  See *Restore Encrypted Virus* on page E-10 for more information.

Version 6.0 Service Pack 1

- **Improved Client Security**

  Prevent malicious software from modifying or terminating important components on the Agent.

- **Ability to Disable the Firewall for All Clients**

  Disable the Firewall for all Clients using the new option on Global Settings.

- **Support for New Operating Systems**

  WFBS now supports Windows 7, Windows Server 2008 R2, and Windows Server 2008 Foundation.

- **Other Enhancements**

  - The installer now queries the Trend Micro servers during installation/upgrade to check the validity of the Activation Code (AC)
  - Improved database migration for Security Servers upgrading from v3.6; this addresses the login error that occurs when querying log files on upgraded servers
  - Updated checking mechanism that ensures the Smart Scan Pattern file is downloaded only when there is sufficient disk space
  - Support for the HTTPS protocol (in addition to the HTTP protocol) for Web Reputation and URL Filtering

Version 6.0 Service Pack 2

- **Low-Impact Smart Scan Pattern Update Mechanism**

  Frequent Smart Scan component updates on the Security Server ensure that Clients scan with the latest patterns. To reduce the impact of updates to Security Server performance, certain resource-intensive processes have been moved to Trend Micro servers in the cloud.

- **Adjustments to Behavior Monitoring and the Firewall for Performance**

  To avoid impacting critical server applications, Behavior Monitoring is now disabled by default on Clients in server groups, while the Firewall remains disabled by default on all Clients. Upgrading to Service Pack 2 automatically disables both features on all Clients in existing server groups. To free system resources, disabling either feature in any group unloads all related drivers and processes. For more information about default feature settings, see *Options for Desktop and Server Groups* on page 6-2.

- **UNC paths on Behavior Monitoring exception list**

  With the Behavior Monitoring exception list supporting UNC paths, you can automatically block or allow programs that run from network folders. For more information about the exception list, see *Using Behavior Monitoring* on page 6-19.

- **Cleanup Mechanism after Updates**

  With Service Pack 2, the Disk Cleaner cleanup tool removes remnant files automatically every time the Security Server updates. By ensuring that unused components do not take up disk space, the tool can free up to 900MB of space. The tool can also be run manually to clean up the Security Server.

- **Other Enhancements**
  - Reduced frequency of security status reporting to Worry-Free Remote Manager to enhance performance
  - Seat count threshold for displaying warnings on the Live Status screen has been changed to 100%
  - Wording changes on the Messaging Security Agent installation screen to cover User Access Control on Windows™ Small Business Server 2008

Version 6.0 Service Pack 3

- **Web Console Updates**
  - The Web console has a drop-down list of shortcuts to common configuration settings so that users can access them easily
  - Security Server displays announcements on the Web console about new patches and updates as they become available
  - Security Server now supports sending email notifications through authenticated SMTP servers
- **New Tools**
  - WFBS includes a password reset tool for the Web management console
  - WFBS now supports the Trend Micro Vulnerability Scanner on 64-bit operating systems
- **Client Updates**
  - Behavior Monitoring supports the cleanup of confirmed fake antivirus files
- **Installation Updates**
  - Support links are now provided on the installation wizard to help users with setup questions
  - Users can now view and customize the directory that installation files are extracted to at the start of the installation process

- **Other Updates**
  - A link to the Trend Micro Worry-Free Knowledge Base is now included in the Microsoft™ Windows™ "Start" menu

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 Web site'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

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 Advanced 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.

The benefits of Smart Scan include:

- **Reduced hardware resources:** only the Scan Server's resources are used for scanning files.

URL Filtering

URL filtering helps you control access to Web sites to reduce unproductive employee time, decrease Internet bandwidth usage, and create a safer work environment. You can choose a level of URL filtering protection or customize which types of Web sites 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 Client/Server Security Agent and Messaging Security Agent
Virus/Malware and Spyware/Grayware transmitted through email messages and spam	POP3 Mail Scan in Client/Server Security Agent and IMAP Mail Scan in Messaging Security Agent Protection for Messaging Security Agent for Microsoft™ Exchange Servers
Network Worms/Viruses	Firewall in Client/Server Security Agent
Intrusions	Firewall in Client/Server Security Agent
Conceivably harmful Web sites/Phishing sites	Web Reputation and TrendProtect in Client/Server Security Agent
Malicious behavior	Behavior Monitoring in Client/Server Security Agent
Fake access points	Transaction Protector in Client/Server Security Agent
Explicit/restricted content in IM applications	IM Content Filtering in Client/Server Security Agent

Components

Antivirus

- **Scan engine (32-bit/64-bit) for Client/Server 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, 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 patterns in the virus pattern file, searching for a match.
- **Virus pattern:** A file that helps the Security Agents identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.
- **Virus cleanup template:** Used by the Virus Cleanup Engine, this template helps identify Trojan files and Trojan processes, worms, and spyware/grayware so the engine can eliminate them.
- **Virus 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.
- **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.

Anti-spyware

- **Spyware scan engine (32-bit):** A separate scan engine that scans for, detects, and removes spyware/grayware from infected computers and servers running on i386 (32-bit) operating systems.
- **Spyware scan engine (64-bit):** Similar to the spyware/grayware scan engine for 32-bit systems, this scan engine scans for, detects, and removes spyware on x64 (64-bit) operating systems.
- **Spyware pattern:** 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 active-monitoring pattern:** Similar to the spyware pattern, 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 threat 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 pattern:** A file that includes the database for all vulnerabilities.

  The vulnerability pattern provides the instructions for the scan engine to scan for known vulnerabilities.

Network Virus

- **Common firewall engine (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.
- **Common 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.
- **WFP driver (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 rating returned by the database and the security level configured, Client/Server 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.

TrendProtect

- **Trend Micro Security database:** TrendProtect 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 Driver:** This driver detects process behavior on clients.
- **Behavior Monitoring Core Service:** CSA 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 patter will be skipped by all policy matches.
- **Behavior Monitoring Detection Pattern:** A pattern containing the rules for detecting suspicious threat behavior.

Transaction Protector

- **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

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

Understanding Threats

Computer security is a rapidly changing subject. Administrators and information security professionals invent and adopt a variety of terms and phrases to describe potential risks or uninvited incidents to computers and networks. 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 damage 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:** Malware is software designed to infiltrate or damage a computer system without the owner's informed consent.
- **Trojans:** A Trojan is a malicious program that masquerades as a harmless application. Unlike virus/malware, Trojans do not replicate but can be just as destructive. 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.
- **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.

The agent programs on the client computers, referred to as the Client/Server 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.

Client/Server 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 a 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 1-15 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

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 Web site. 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

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.

Messaging Security Agents can detect mass-mailing attacks during Antivirus scanning. The default action that is set for mass-mailing behavior takes precedence over all other actions. The Trend Micro recommended action against mass-mailing attacks is *delete entire message*.

Product Component Terminology

The following table defines the terms that appear in the product documentation:

TABLE 1-2. Product Component Terminology

ITEM	DESCRIPTION
Security Server	The Security Server hosts the Web console, the centralized Web-based management console for the product.-A
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.
Agent/CSA/MSA	The Client/Server Security Agent or Messaging Security Agent. Agents protect the client it is installed on.
Client	Clients are Microsoft Exchange servers, desktops, portable computers, and servers where a Messaging Security Agent or a Client/Server Security Agent is installed.
Web console	The Web console is a centralized, Web-based, management console that manages all the Agents. The Web console resides on the Security Server.

Chapter 2

Preparing for Installation

The steps in this phase help you develop a plan for WFBS 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 2-26 for more information.
3. Identifying the number of clients. Refer to *Identifying the Number of Clients* on page 2-26 for more information.
4. Planning for network traffic. Refer to *Planning for Network Traffic* on page 2-27 for more information.
5. Determining desktop and server groups. Refer to *Determining the Number of Desktop and Server Groups* on page 2-29 for more information.
6. Choosing installation/deployment options for Client/Server Security Agents. Refer to *Choosing Deployment Options for Agents* on page 2-29 for more information.

Phase 2: Installing 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: Update the System Checklists section of the WFBS *Administrator's Guide*. Reference this information while installing WFBS.

2. Installing or upgrading WFBS. Refer to *Installation Overview* on page 2-20 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 Client/Server Security Agent on all the servers and desktops and install Messaging Security Agent on the Exchange servers. This phase includes the following tasks:

Note: Refer to *Agent Installation Overview* on page 3-2 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 Client/Server Security Agent on Clients, customize the default settings if required. This includes the following tasks:

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

Server and Agent System Requirements

To install WFBS Security Server (which includes the scan server) and agent, the following are required:

Note: Client/Server Security Agent supports Citrix Presentation Server™ 4.0/4.5/5.0 and Remote Desktop.
This version supports VMware® ESX™ 3.0/3.5, VMWare Server 1.0.3/2.0.1, WMware Workstation 6.0/6.5, and Microsoft Hyper-V™ Server 2008.

TABLE 2-3. 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 minimum, 2GB recommended • 512MB minimum (x86 systems); 1GB recommended • 1GB (x64 systems); 2GB recommended • 4GB (Windows™ Essential Business Server 2008 or Windows™ Small Business Server 2008 systems)
Disk space	6GB total disk space (excludes MSA and CSA disk usage) • 2GB for installation • 4GB for operation

TABLE 2-3. System Requirements (Continued)

Item	Minimum Specifications	
Operating system	**Series or Family**	**Supported Service Packs or Releases**
	Windows 2000	SP3 or SP4
	Windows Small Business Server (SBS) 2000	No service pack or SP1a
	Windows XP	SP2 or SP3
	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 Vista™	SP1 or SP2
	Windows Home Server	No service pack or SP1
	Windows Server 2008 R2	No service pack
	Windows Server 2008	SP1 or SP2
	Windows SBS 2008	SP1 or SP2
	Windows 2008 Foundation	SP1 or SP2
	Windows Essential Business Server (EBS) 2008	SP1 or SP2
	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.	

TABLE 2-3. System Requirements (Continued)

Item	Minimum Specifications
Web server	• Microsoft™ Internet Information Server (IIS) 5.0 (Windows 2000 or SBS 2000) • 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. Apache must be used on these operating systems. If you have an Apache server already installed, Trend Micro recommends uninstalling it. An Apache server will be installed with the Security Server.
Web Console	
Web browser	Internet Explorer 6.0 or later (32-bit only)
PDF reader (for reports)	Adobe™ Acrobat™ Reader 4.0 or later
Display	High-color display with resolutions of 1024x768 or higher
Client/Server 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 2000, SBS 2000, XP, Server 2003, SBS 2003, or Home Server)

TABLE 2-3. System Requirements (Continued)

Item	Minimum Specifications
Memory	• 4GB (SBS/EBS 2008) • 1GB minimum; 2GB recommended (Windows Server 2008, SBS 2000 or 2003) • 512MB minimum; 1GB recommended (Windows Vista, Windows 7) • 512MB minimum; 1GB recommended (Windows 2000 Server, Server 2003, or Home Server) • 256MB minimum; 512MB recommended (Windows 2000, Windows XP)
Disk space	450MB total disk space • 300MB for installation • 150MB for operation
Operating System	The Client/Server Security Agent supports all operating systems supported by the Security Server. In addition to these operating systems, the CSA also supports: • Windows XP Tablet PC (SP2 or SP3) • Windows XP Home (SP2 or SP3) • Windows 7 (**Note:** Windows 7 Starter edition is not supported)
Web browser (for Web-based setup)	Internet Explorer 6.0 or later
Display	256-color display or higher with resolutions of 800x600 or higher

TABLE 2-3. 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	1.6GB total disk space • 800MB for installation • 800MB for operation	
Operating system	**Series or Family**	**Supported Service Packs or Releases**
	Windows 2000 (Server and Advanced Server only)	SP4
	Windows SBS 2000	No service pack or SP1a
	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 SBS 2008	SP1 or SP2
	Windows EBS 2008	SP1 or SP2
	Note: All major editions and 64-bit versions of these operating systems are supported unless noted otherwise.	

TABLE 2-3. System Requirements (Continued)

Item	Minimum Specifications
Web server	• IIS 5.0 (Windows 2000 or SBS 2000) • IIS 6.0 (Windows Server 2003, SBS 2003, or Home Server) • IIS 7.0 (Window Server 2008, SBS 2008, or EBS 2008) • Apache HTTP Server ™ HTTP Server 2.0.63 or later
Mail server	Exchange Server 2000 SP2 or SP3, 2003 SP1 or SP2, or 2007 no service pack or SP1 **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.

Note: CSA supports Gigabit network interface cards (NICs).

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

Note: 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 ensure that client-server communication can be established.

Choosing Your Edition

Full Version and Evaluation Version

You can install either a full version of WFBS or a free, evaluation version.

- **Full version:** Comes with technical support, virus pattern downloads, real-time scanning, and program updates for one year. You can renew a full version by purchasing a maintenance renewal. You need an Activation Code to install the full version.
- **Evaluation version:** Provides real-time scanning and updates for 30 days. You can upgrade from an evaluation version to a full version at any time. You do not need an Activation Code to install the evaluation version.
    - **With or without Email Reputation Services:** you can choose to include or exclude Email Reputation Services (ERS) in the evaluation version. ERS is a Trend Micro hosted anti-spam solution.

Registration Key and Activation Codes

Your version of WFBS comes with a Registration Key. During installation, WFBS prompts you to enter an Activation Code.

If you do not have the Activation Code(s), use the Registration Key that came with your product to register on the Trend Micro Web site and receive the Activation Code(s). The WFBS installer can automatically redirect you to the Trend Micro Web site:

http://www.trendmicro.com/support/registration.asp

You can still install an evaluation version without the Registration Key or Activation Code. To find out more information contact your Trend Micro sales representative (see *Contacting Trend Micro* on page B-4).

Worry-Free Business Security Advanced includes both a software component and hosted email services. No Activation Code is necessary to install just the software component; however, you need a trial Activation Code to install the evaluation software with Email Reputation Services (ERS) or evaluate Trend Micro Hosted Email Security. Sign up for an evaluation Registration Key to obtain an Activation Code by visiting here: https://trial.securecloud.com/wfbs/.

Note: If you have questions about registration, please consult the Trend Micro Web site at the following address:
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 2-4. Features Available by Product Editions

Features	Worry-Free Business Security	Worry-Free Business Security Advanced
Component Updates	Yes	Yes
Antivirus/Anti-spyware	Yes	Yes
Firewall	Yes	Yes
Web Reputation	Yes	Yes
Behavior Monitoring	Yes	Yes
TrendSecure	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

TABLE 2-4. Features Available by Product Editions (Continued)

Features	Worry-Free Business Security	Worry-Free Business Security Advanced
Email Message Content Filtering	No	Yes
Attachment Blocking	No	Yes
URL Filtering	Yes	Yes

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

TABLE 2-5. License Status Consequences

	Fully Licensed	Evaluation (30 days)	Expired
Expiration Notification	Yes	Yes	Yes
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.

License and Maintenance Agreement

When you purchase Worry-Free Business Security or Worry-Free Business Security Advanced, you receive a license for the product 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 maintenance for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro then-current 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 virus pattern file, 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 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, or on the Trend Micro Online Registration URL:

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

License Versions

Trend Micro provides different versions of Worry-Free Business Security and Worry-Free Business Security Advanced. Each version uses a different Activation Code.

- **Worry-Free Business Security:** Designed to protect the desktops, laptops, and server computers on your local network. Includes Outbreak Defense, Firewall, and Antivirus and Anti-spyware scanning.
- **Worry-Free Business Security Advanced:** Designed to protect the Microsoft Exchange servers on your local network. Includes all the features of Worry-Free Business Security for SMB plus Anti-spam, Content Filtering, and Attachment Blocking.
- **Worry-Free Business Security Advanced Evaluation Version (with or without email Reputation Services):** Test all the features of Worry-Free Business Security Advanced for SMB for a 30-day evaluation period. When the evaluation period ends the Security Server no longer receives updated components. By default, if no Activation Code was entered during installation, the evaluation version is installed.

Consequences of an Expired License

When a fully licensed version Activation Code expires, you can no longer download the 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.

Protecting Your Network

WFBS protection consists of the following components:

- **The Web 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.
- **Client/Server Security Agent:** protects Windows Vista/2000/XP/Server 2003/Server 2008 computers from virus/malware, spyware/grayware, Trojans, and other threats.
- **Messaging Security Agent:** which protects Microsoft Exchange servers, filters spam, and blocks content.
- **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.

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.

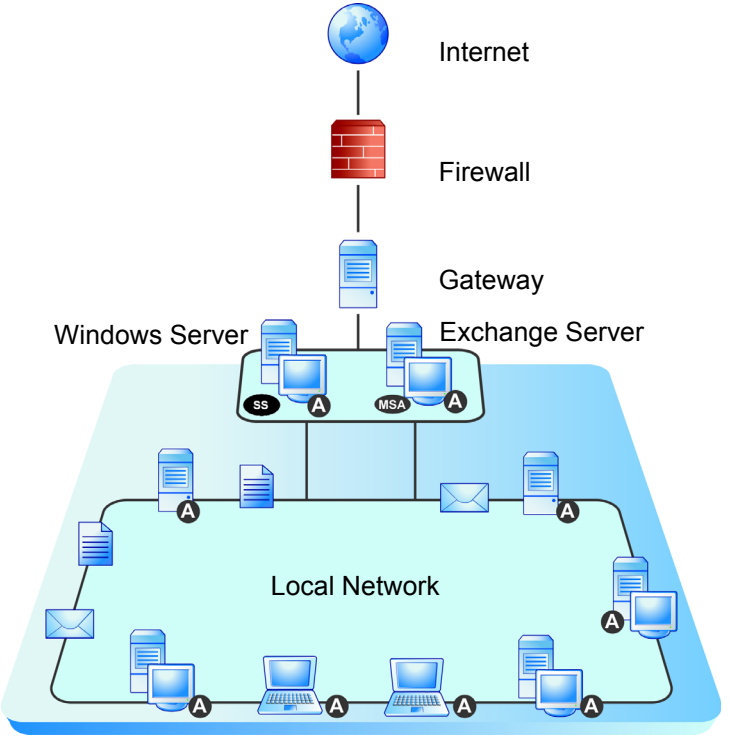

FIGURE 2-1. Network topology example

TABLE 2-6. Network Topology Example Descriptions

SYMBOL	DESCRIPTION
A	Client/Server 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. 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/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 console, the centralized Web-based management console for WFBS. 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 agents.

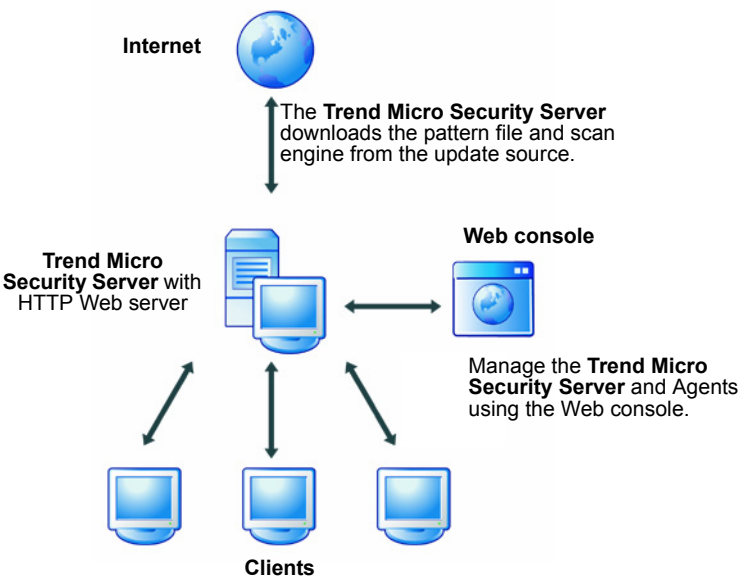

FIGURE 2-2. How Client/Server communication through HTTP works

Client/Server Security Agent

The Client/Server Security Agent (indicated by **A** in *Figure 2-1*) reports to the Trend Micro 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 Client/Server 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.

Scan Server

As part of the Smart Protection Network, WFBS now provides the ability to scan your clients with a Scan Server. This takes the burden of downloading components and scanning client computers off your clients 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 agents and as a scanner.
- **Trend Micro 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 your protection.

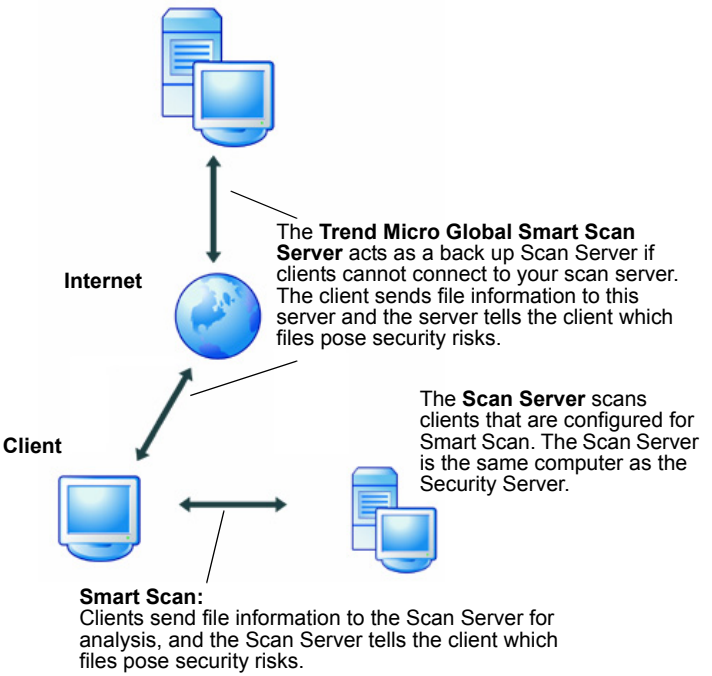

FIGURE 2-3. How Smart Scan communication works

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 installer 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 directory 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 Client/Server Security Agent.
- **Client software installation path:** Configure the client installation path where Client/Server 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 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 (such as typically implemented for Windows 2000 server with IIS 5.0), 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 Web site:** The same port number as your HTTP server's TCP port.
  - **IIS server virtual Web site:** 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 2-7*:

TABLE 2-7. 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! Many hacker and virus attacks use HTTP and are directed 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 agents are using to connect to the scan server, open `SSCFG.ini` in the directory where the server is installed.

Trend Micro Security Server Prescan

Before the installer begins the installation process, it performs a prescan. This prescan includes a virus scan and Damage Cleanup Services scan to help ensure the target computer does not contain viruses, 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 viruses)
- the Windows folder
- the Program Files folder

Actions for Prescan Detections

If the WFBS setup program detects viruses, Trojans, or other potentially malicious code, you can take the following actions:

- **Clean:** Cleans an infected file by removing the virus or malicious application. WFBS encrypts and renames the file if the file is uncleanable.
- **Rename:** Encrypts the file and changes the file extension to VIR, VIR1, VIR2, and so on. The file remains in the same location. Refer to the WFBS *Administrator's Guide* to decrypt a file encrypted by WFBS.

- **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 Client/Server Security Agent program. If using an IIS Web server, the setup program automatically stops and restarts the IIS/Apache service during Web server installation.

WARNING! Make sure that you do not install the Web 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 effect 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/disk resource.

Notes for Windows SBS and EBS 2008 Users

Due to incompatibilities between WFBS and the security features provided with Windows Small Business Server (SBS) 2008 or Windows Essential Business Server (EBS) 2008, the following will occur during installation:

- The installer will prevent you from installing the Messaging Security Agent on a computer with Microsoft Forefront Security for Exchange Server (Forefront). The installer will display corresponding messages when Forefront is detected on the target computer.
- The Client/Server Security Agent (CSA) installation will automatically remove the Microsoft OneCare client from target computers.

Trend Micro strongly recommends that you install the Security Server on Windows EBS computers with the Management Server role. On these servers, the EBS console add-in is automatically installed with the Security Server. Likewise, install the Messaging Security Agent on computers with the Messaging Server role.

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 proper Trend Micro Security Server installation and performance.

Note: WFBS cannot uninstall the server component of any third-party antivirus product but can uninstall the client component (see *Migrating from Other Antivirus Applications* on page 4-5 for instructions and for a list of third-party applications WFBS can remove).

Security Applications in EBS and SBS 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.

CSA and OneCare

Although the Security Server can be installed with Microsoft Windows Live™ OneCare for Server, the Client/Server Security Agent (CSA) cannot be installed with the OneCare client. The CSA installer will automatically remove OneCare from client computers.

Databases

You can scan databases; however, this 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 Vista, Windows XP SP2, 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 2-21 for information on listening ports and see 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 Client/Server 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 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 Client/Server Security Agent or 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 2000, XP, Server 2003 or Vista, 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 Agents* on page 2-29.

Note: A single Security Server installation can manage up to 2500 clients. If you have more clients than this, 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 who are configured for Smart Scan
- Sending feedback to the Trend Micro Smart Protection Network

Clients generate traffic when:

- Starting up
- Shutting down
- Generating logs
- Switching between roaming mode and normal mode
- Performing scheduled updates
- Performing manual updates ("Update Now")
- Connecting to the Scan Server for Smart Scan

Note: Other than 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 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, which is approximately 5KB to 200KB. The full pattern is approximately 20MB when compressed and takes substantially longer to download.

Trend Micro releases new pattern files daily. However, if a particularly damaging virus 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, application server), Trend Micro recommends that you install 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 Server Agent
```

Determining the Number of Desktop and Server Groups

Every Client/Server 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 Agents

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

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. Client/Server 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, Remote Install and Login Script Setup are recommended. Remote-install and login-script setups do not require administrative privileges to be assigned 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 Vista/2000/XP (Professional Edition only) and Server 2003.

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

WFBS includes a tool called the Vulnerability Scanner, which can help you detect computers that are not protected by WFBS. Once Vulnerability Scanner detects an unprotected computer, it deploys Client/Server 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: To install Client/Server 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 Client/Server 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 2-8. Port Checklist

PORT	SAMPLE	YOUR VALUE
SMTP	25	
Proxy	Administrator Defined	
Security Server: Non-SSL Port	8059	
Security Server: SSL Port	4343	
Client/Server Security Agent	21112	
Messaging Security Agent	16372	
Scan Server SSL Port	4345	
Scan Server Non-SSL Port	8082	

Security Server Address Checklist

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

TABLE 2-9. 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	

TABLE 2-9. Server Address Checklist (Continued)

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

The topics discussed in this chapter include:

Installation Overview

There are three methods for installing WFBS:

- **Typical:** Provides a simple and 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.
- **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 the WFBS. See *Upgrading the Client/Server Security Agent starting on page 4-9* on page 4-1 for instructions.

Note: If information from a previous 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 WFBS server, the Scan Server is automatically installed. You do not need to choose to install the Scan Server or 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**
  - **Web Site:** OfficeScan
  - **Default URL:** `https://<IP_ADDRESS>:4343/SMB`
- **Client/Server Security Agent settings:** Refer to the WFBS *Administrator's Guide* for information.

To perform an installation using the Typical method follow the steps in *Custom Installation Walkthrough* on page 3-3 ignoring 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 Web console. Refer to *Part 2: Server and Web Console Settings* on page 3-10.
3. Configure the Client/Server Security Agent and Messaging Security Agent installation options. Refer to *Part 3: Agent Installation Options* on page 3-22.

4. Start the installation process. Refer to *Part 4: Installation Process* on page 3-28.
5. **Optional.** Configure the Remote Messaging Security Agent installation option for remote Exchange servers. Refer to *Part 5: Remote Messaging Security Agent Installation* on page 3-29.

Part 1: Pre-configuration Tasks

The pre-configuration tasks consist of launching the installation wizard, providing licensing and activation details, prescanning the server for viruses, 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 **Product Activation** screen appears.

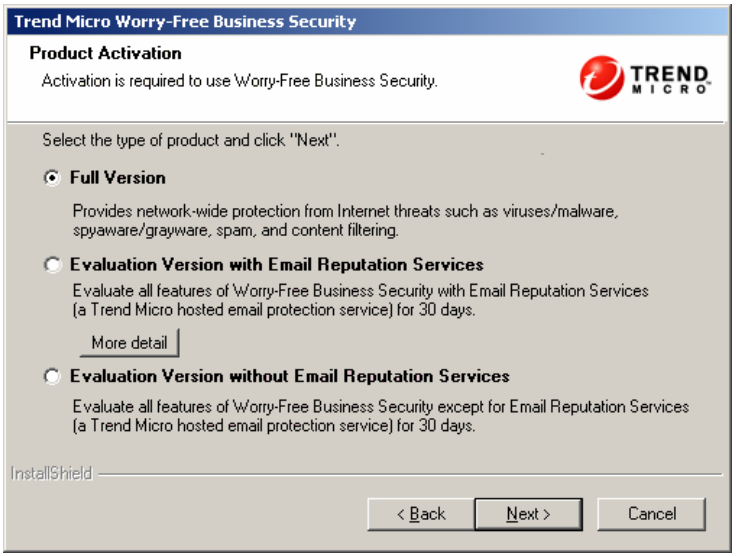

FIGURE 3-1. Product Activation screen

5. From the **Product Activation** screen, choose one of the following options and click **Next**:
   - **Full Version**
   - **Evaluation Version with Email Reputation Services:** Refer to:

     http://us.trendmicro.com/us/products/enterprise/network-reputation-services/

     for more information about Email Reputation Services.
   - **Evaluation Version without Email Reputation Services**

Note: You need an Activation Code or Registration Key to install the full version and to install the evaluation version with Email Reputation Services.

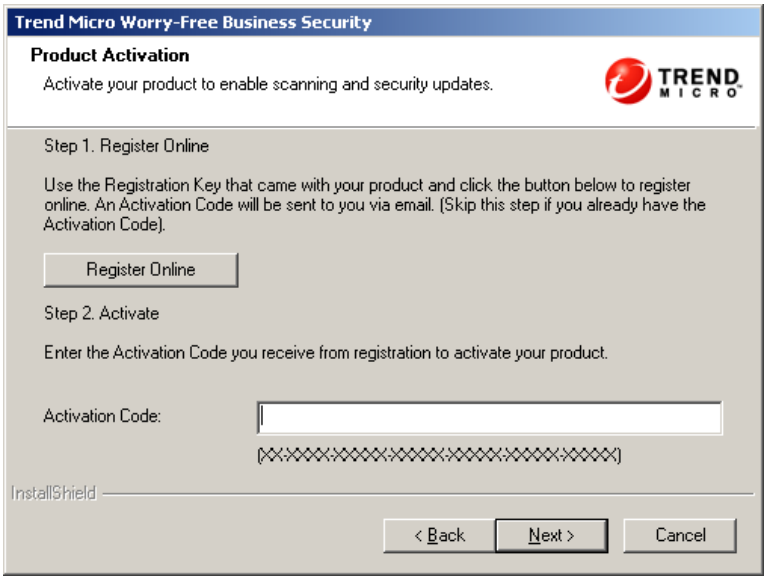

FIGURE 3-2. Product Activation screen

6. Click **Register Online** if WFBS has not been registered yet. A browser window opens. Follow the instructions on the **Registration** screen.
7. Type the Activation Code in the **Activation Code** field.

Note: If you do not have an **Activation Code**, click **Next** to install the evaluation version. Upgrade to the full version before the 30-day evaluation period ends and all settings will remain.

---

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

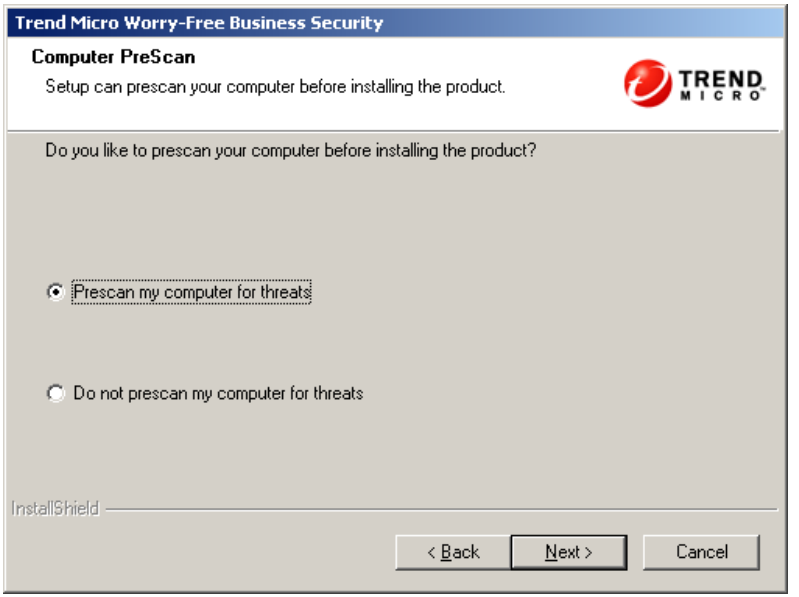

FIGURE 3-3. Computer Prescan screen

9. Choose whether to prescan your computer for threats by selecting one of the following options:
   - **Prescan my computer for threats**
   - **Do not prescan my computer for threats**
   - Trend Micro highly recommends prescanning your computer for security threats. Not prescanning the computer could prevent successful installation.

Note: If you choose to prescan your computer for threats, a threat progress screen will appear while scanning is taking place.

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

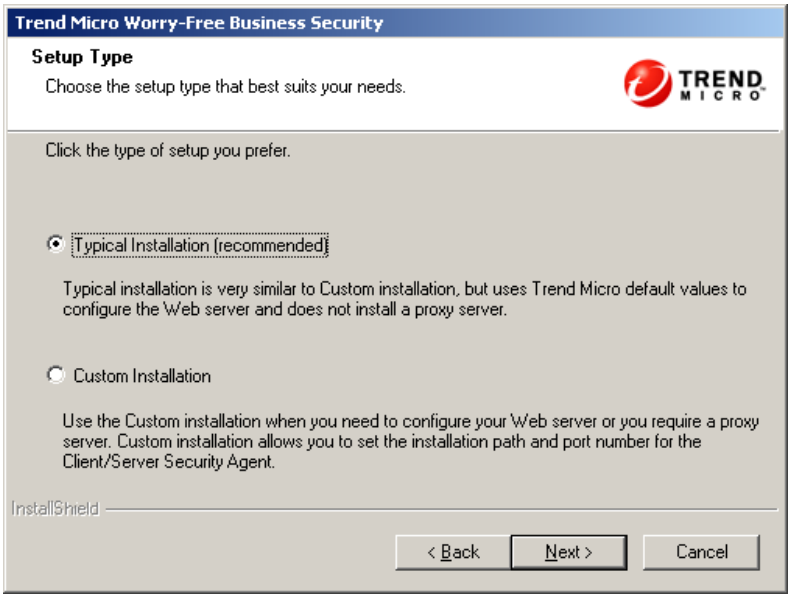

FIGURE 3-4. Setup Type screen

11. From the **Setup Type** screen, choose one of the following options:
    - **Typical installation (recommended)**
    - **Custom installation**

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

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

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

    This completes all pre-installation tasks.

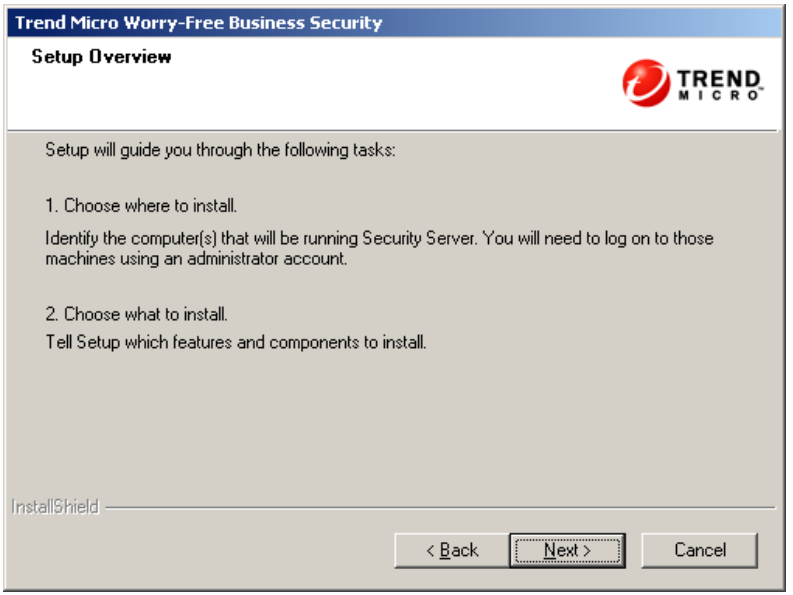

FIGURE 3-5. Installation Setup Overview screen

13. The **Setup Overview** screen briefly lists the tasks that you need to complete in order to install the Trend Micro Security Server, Web console, Messaging Security Agent, and Client/Server Security Agent.

Part 2: Server and Web Console Settings

To configure the Security Server and Web console:

1. From the **Setup Overview** screen, click **Next**. The **Installation Stage** screen appears with the Security Server icon highlighted.

FIGURE 3-6. Security Server Installation Stage screen

2. Click **Next**. The **Server Identification** screen appears.

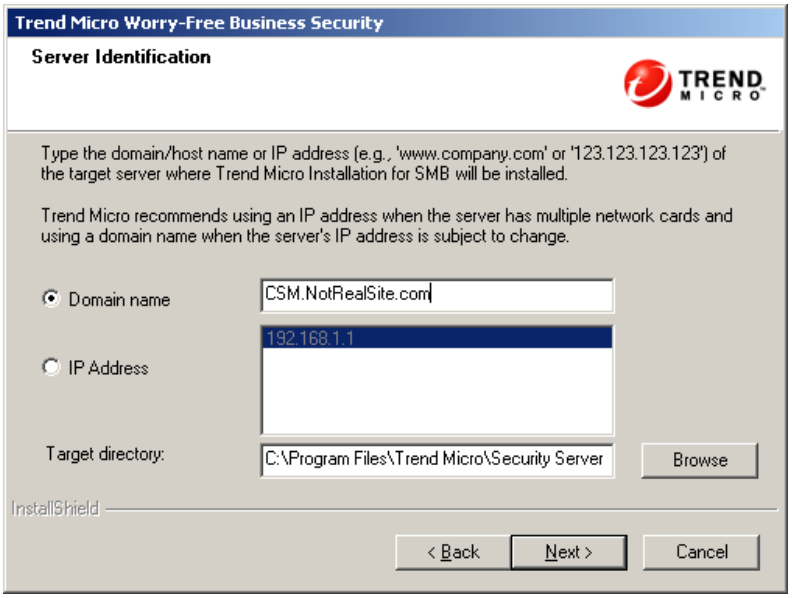

FIGURE 3-7. Server Identification screen

3. Choose from one of the following server identification options for client-server communication:
   - **Server information:** Choose Domain name or IP address:
     - **Domain name:** Verify the target server's domain name. You can also use the server's fully qualified domain name (FQDN) if necessary to ensure successful client-server communication.
     - **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 or FQDN, instead of the IP address.

   - **Target directory.** Specify the target directory where Trend Micro Security Server will be installed.

4. Click **Next**. The **Select Program Folder** screen appears.

FIGURE 3-8. Select Program Folder screen

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

5. Type a location in the **Program folder** field where program shortcuts will be stored or accept the default location.
6. Click **Next**. The **Web Server** screen appears allowing you to choose a Web server.

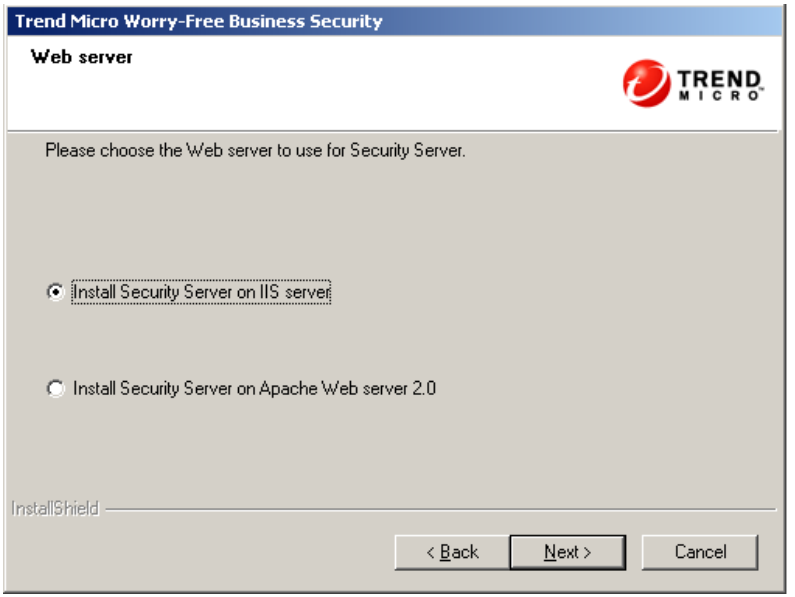

FIGURE 3-9. Web Server screen

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

7. From the **Web Server** screen, select a Web server to host the Web console. Choose from one of the following:
   - IIS server
   - Apache Web server
8. Click **Next**. Depending on the type of server chosen, the corresponding screen appears.

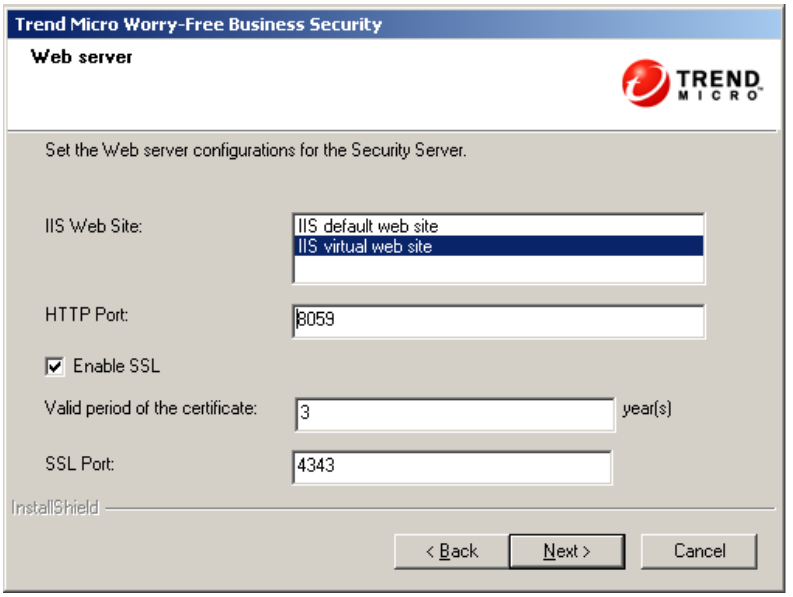

FIGURE 3-10. IIS Web Server Configuration screen

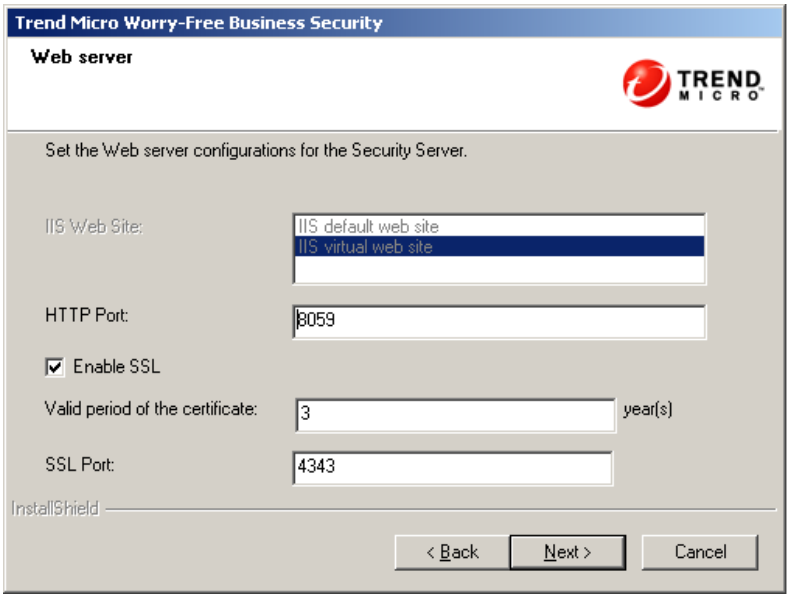

FIGURE 3-11. Apache Web Server Configuration screen

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

---

9. Configure the following Web server settings:
   - **HTTP port**
   - **Enable SSL**
   - **Valid period of the certificate**
   - **SSL port**

Note: If using IIS server, you must specify an IIS Web site, **virtual** or **default**. WFBS will assign default values for the HTTP and SSL port settings for using the IIS default Web site.

---

10. Click **Next**. The **Proxy Server** screen appears.

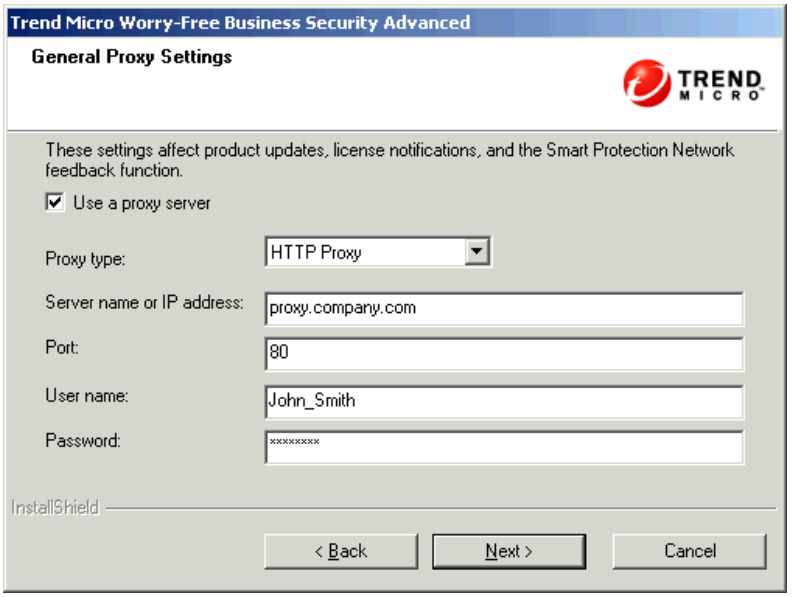

FIGURE 3-12. Proxy Server screen

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

11. If a proxy server is required to access the Internet, select the **Use a proxy server** check box and then provide the following information:
    - **Proxy type**
    - **Server or name IP address**
    - **Port**
    - **User name:** Provide only if the server requires authentication.
    - **Password:** Provide only if the server requires authentication.
12. Click **Next**. A proxy server settings screen for Web Reputation and Behavior Monitoring appears.

These client services use the proxy server and port specified in Internet Explorer. If that proxy server requires authentication, use this screen to specify logon credentials.

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

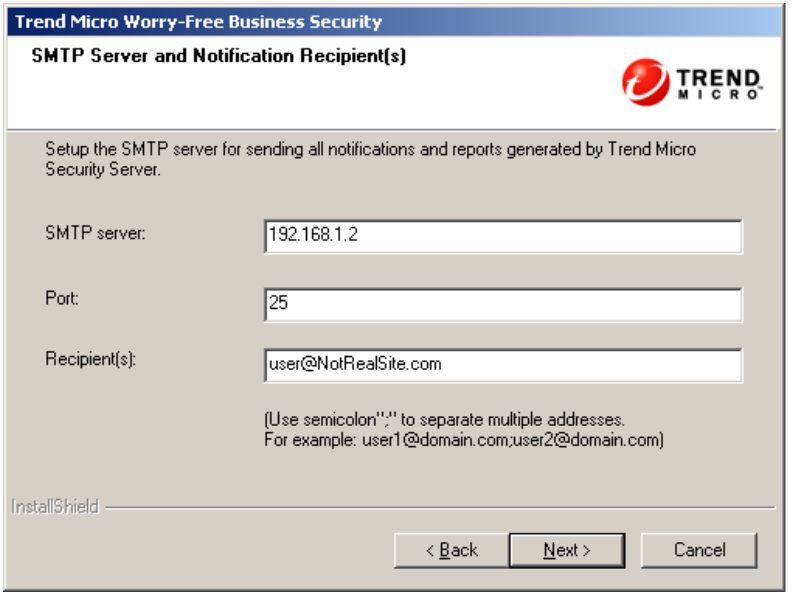

FIGURE 3-13. SMTP Server and Notification Recipient(s) screen

14. The **SMTP Server and Notification Recipient(s)** screen requires the following information:
    - **SMTP server**: the mail server
    - **Port**
    - **Recipient(s)**

    Note: If the SMTP server (mail 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.

    Refer to your ISP mail server settings. If you do not know these settings, progress to the next step. These settings can be configured at another time.

    Tip: You can update the SMTP settings after installation. Refer to the Administrator's Guide for instructions.

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

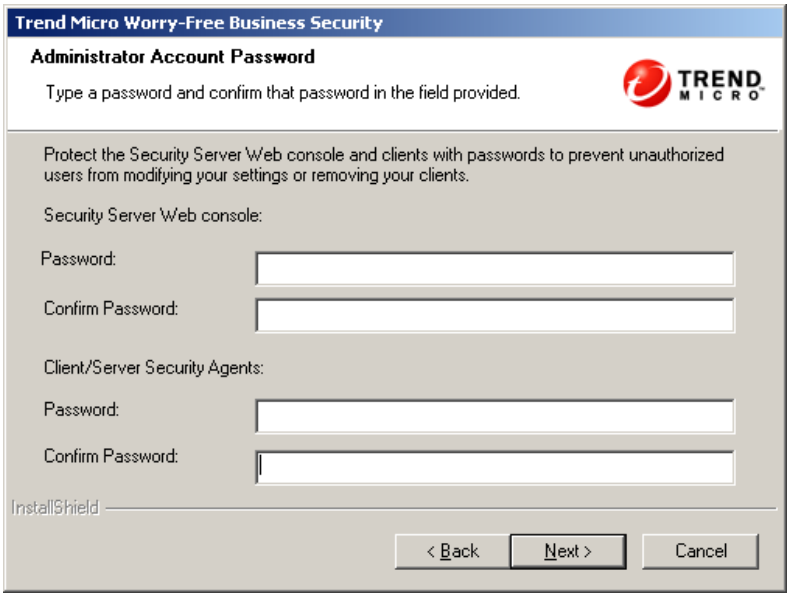

FIGURE 3-14. Administrator Account Password screen

16. The **Administrator Account Password** screen requires the following information:
    - **Security Server Web console:** Required to log on to the Web console.
        - **Password**
        - **Confirm password**
    - **Client/Server Security Agents:** Required to uninstall the Client/Server Security Agents.
        - **Password**
        - **Confirm password**

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

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

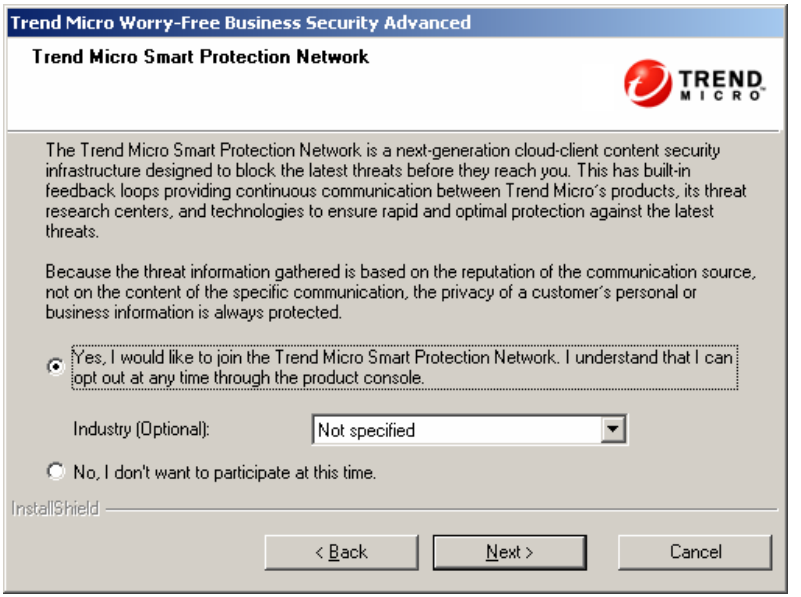

FIGURE 3-15. Trend Micro Smart Protection Network screen

18. Choose whether to participate in the Trend Micro Smart Protection Network feedback program. You can choose to cancel participation through the Web console later.
19. Click **Next**. The **Component Selection** screen appears.

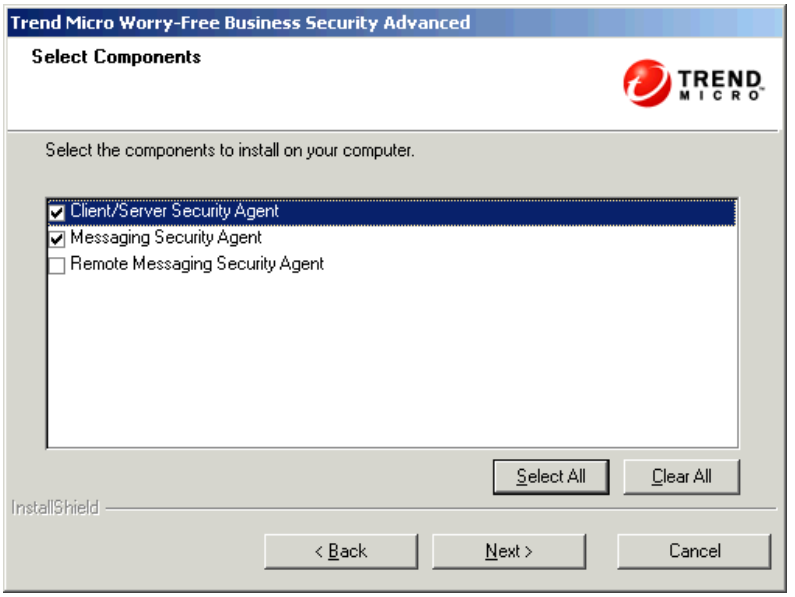

FIGURE 3-16. Component Selection screen

20. Select one of the following:

- **Client/Server Security Agent:** the agent that protects desktops/servers
- **Messaging Security Agent:** the agent that protects Microsoft Exchange servers (installed locally on this computer)
- **Remote Messaging Security Agent:** the agent that protects other Microsoft Exchange servers (this will perform a remote install)

Note: The first MSA installation option (local installation) will only be available on computers with supported versions of Exchange Server. If this option is not available, ensure that the Microsoft Exchange Information Store service is started and that the computer does not have Microsoft Forefront Security for Exchange Server (Forefront) installed.

---

21. Click **Next**. The **Messaging Security Agent Installation Stage** screen appears with the Messaging Security Agent icon highlighted.

FIGURE 3-17. Messaging Security Agent Installation Stage screen

Note: If the server does not have Exchange server on it, the Messaging Security Agent option will be unavailable.

Part 3: Agent Installation Options

The options below are dependant upon the components selected from the Component Selection screen. For example, if the local server already has the Client/Server Security Agent installed, the option to install and configure the Client/Server Security Agent will not appear. If the local server does not have an Exchange server installed on it, the option to install and configure the Messaging Security Agent will also be unavailable.

To configure the Messaging Security Agents and Client/Server Security Agents:

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

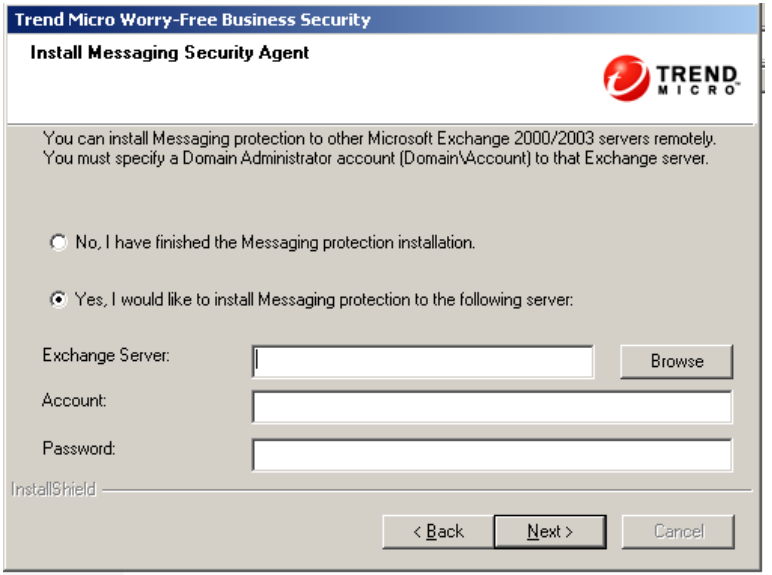

FIGURE 3-18. Install Messaging Security Agent screen

2. Select to install Messaging protection and enter the following for the Domain Administrator account:
   - **Exchange Server**
   - **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.

---

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

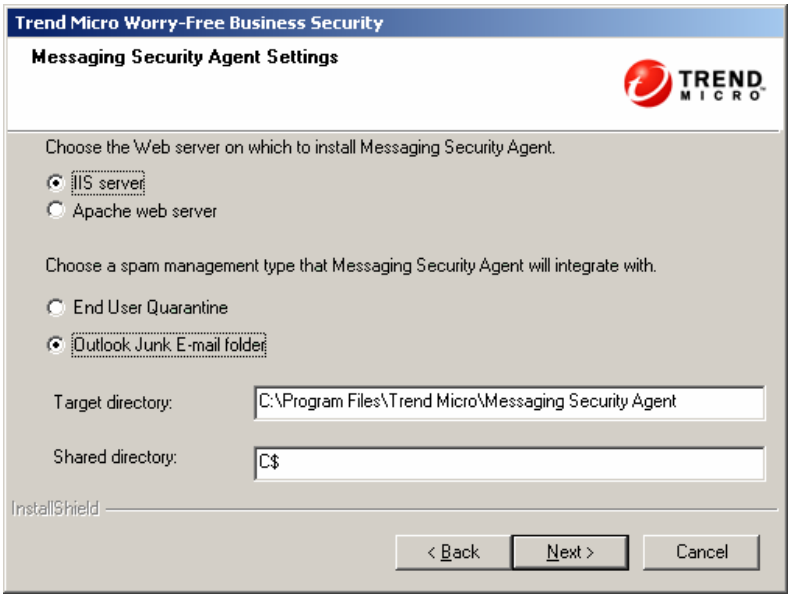

FIGURE 3-19. Messaging Security Agent Settings screen

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

4. From the **Messaging Security Agent Settings** screen, configure the following;:
   - Web server
     - **IIS server**
     - **Apache Web server**
   - 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 E-mail folder:** if selected, WFBS saves 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, it is recommended that this option is selected

Note: The option to select between EUQ and the Junk E-mail folder is only available if the computer is running Exchange Server 2003. The Junk E-mail feature is not supported by Exchange Server 2000. On Exchange Server 2007, EUQ fully integrates with the Junk E-mail feature.

- **Target directory:** Directory where the Remote Messaging Security Agent files are installed.
- **Shared directory:** System root directory for the Remote Messaging Security Agent installation.

Note: Anonymous Access is required for communication between the Security Server and the Messaging Security Agent. The installation program will automatically enable Anonymous Access Authentication Methods for the Messaging Security Agent. To view the Anonymous Access Authentication Methods, access the settings for Messaging Security Agent Web site on IIS.

5. Click **Next**. The **Client/Server Security Agent Installation Stage** screen appears with the Client/Server Security Agent and Remote Client/Server Security Agent icons highlighted.

FIGURE 3-20. Client/Server Security Agent Installation Stage screen

---

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

---

6. Click **Next**. The **Client/Server Security Agent Installation Path** screen appears.

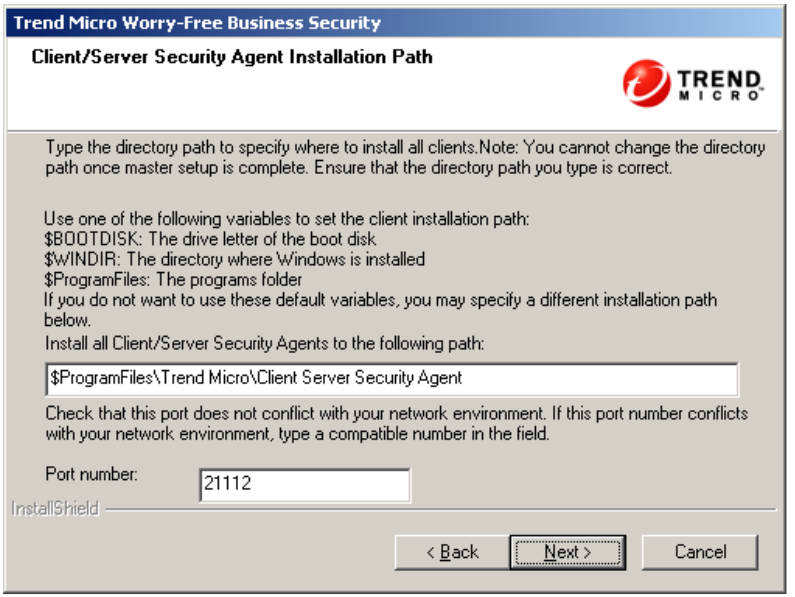

FIGURE 3-21. Client/Server Security Agent Installation Path screen

---

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

---

7. Set the following items:
   - **Path:** The directory where the Client/Server Security Agent files are installed.
   - **Port number:** The port used for Client/Server Security Agent and Security Server communications.

Note: The Client/Server Security Agent applies the Path and Port settings to both local and remote clients.

---

8. Click **Next**. The **Start Copying Files** screen appears.

Part 4: Installation Process

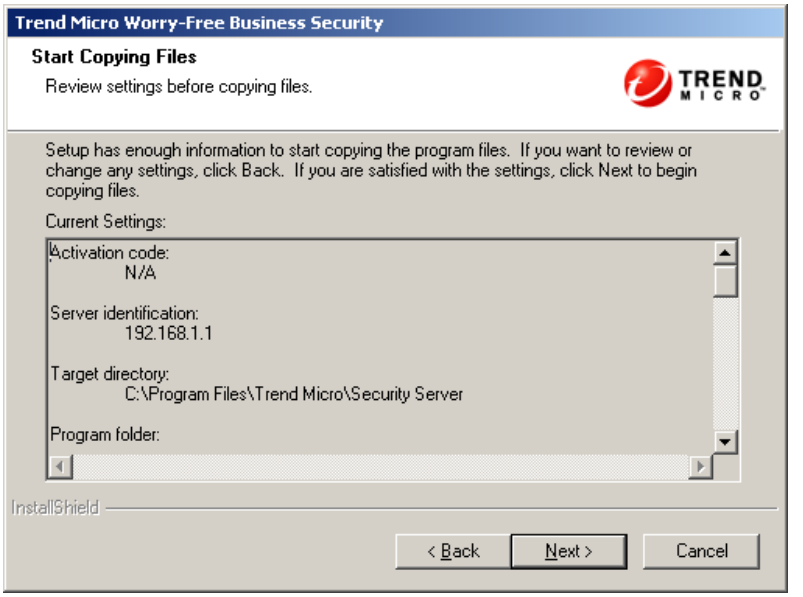

FIGURE 3-22. Start Copying Files screen

1. Click **Next**. The installation process begins installing the Security Server, Messaging Security agent, and Client/Server Security Agent. Upon completion, the **Remote Messaging Security Agent Installation Stage** screen appears.

Note: The next step assumes that you selected install Remote Messaging Security Agent from the Component Selection screen. If you chose not to select the option to install the Remote Messaging Security Agent, an InstallShield Wizard Complete screen will appear.

Part 5: Remote Messaging Security Agent Installation

To install the Remote Messaging Security Agent:

1. The **Remote Messaging Security Agent Installation Stage** screen appears.

FIGURE 3-23. Remote Messaging Security Agent Installation Stage

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

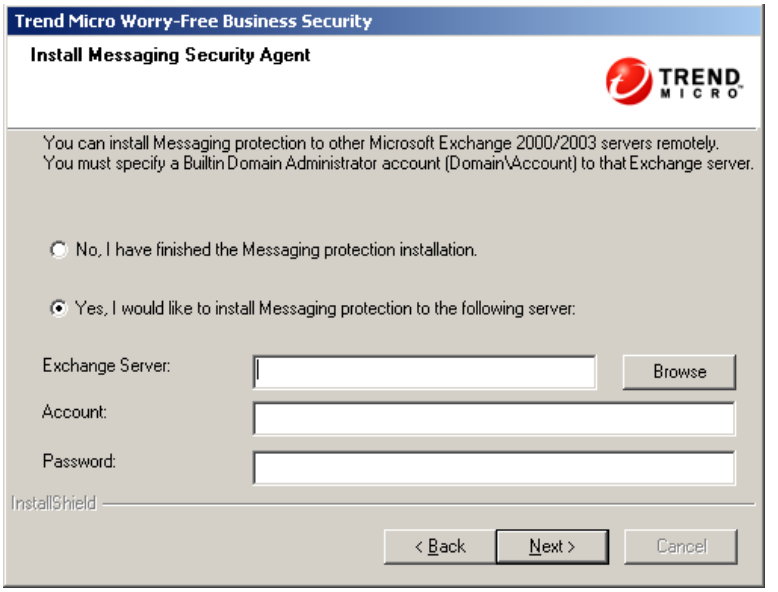

FIGURE 3-24. Install Messaging Security Agent screen

3. To install messaging protection to a remote Exchange server, click **Yes** and then enter credentials for the builtin domain administrator account.

Note: If you choose No, the InstallShield Wizard Complete screen will appear, and the installation process will be complete. If you choose Yes, upon completion of the Remote Messaging Security Agent installation, you will be prompted to install another Remote Messaging Security Agent.

Provide the following information:

- **Exchange Server:** IP address or machine name
- **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.

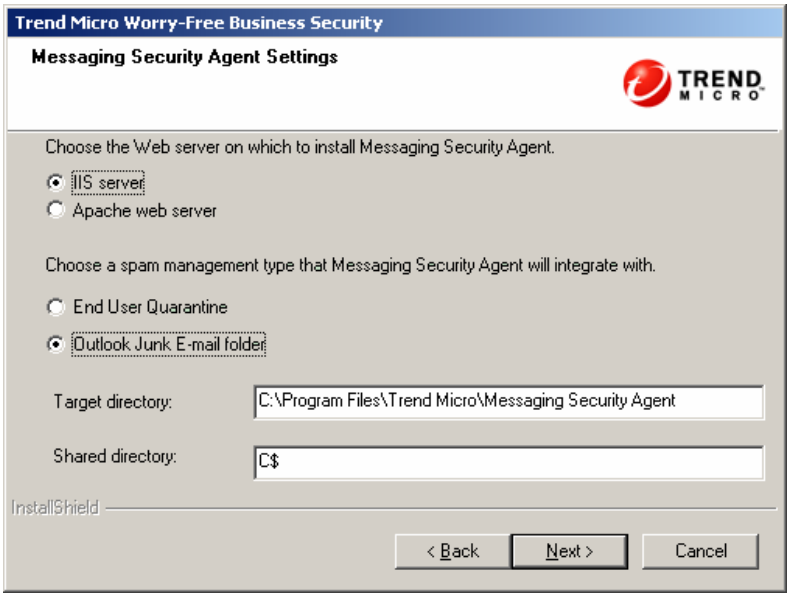

FIGURE 3-25. Messaging Security Agent Settings screen

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

5. From the Remote Messaging Security Agent Settings screen, update the following as required:
   - Web server
     - **IIS server**
     - **Apache Web server**
   - 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 E-mail folder:** if selected, WFBS saves 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, it is recommended that this option is selected

Note: The option to select between EUQ and the Junk E-mail folder is only available if the computer is running Exchange Server 2003. The Junk E-mail feature is not supported by Exchange Server 2000. On Exchange Server 2007, EUQ fully integrates with the Junk E-mail feature.

- **Target directory:** Directory where the Remote Messaging Security Agent files are installed.
- **Shared directory:** System root directory for the Remote Messaging Security Agent installation.

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.

Silent Installation Walkthrough

Use Silent installation to help you run multiple identical installations on separate networks. The procedure for running a silent installation is identical to the Custom installation except for the following pre-configuration and actual installation steps.

Pre-configuration steps:

1. In the command prompt, go to the directory where the WFBS setup files are located.
2. At the prompt, type **setup -r**.
3. To continue with the setup process and to learn more about configuring WFBS during installation, see *Custom Installation Walkthrough* on page 3-3.

   A confirmation message is displayed at the end of the installation.

Starting the silent installation:

1. Go to:
   - **Windows 2000:** C:\WINNT
   - **Windows XP/2003:** C:\Windows
   - **Vista:** C:\Windows
2. Find the file **setup.iss** and copy it to the WFBS setup folder.
3. Open a command window and at the prompt, go to the WFBS setup folder and type **setup -s**.

To verify that the installation is successful, go to the WFBS folder and view the `setup.log` file. If `ResultCode=0`, the installation was successful.

Verifying the Installation

After completing the installation or upgrade, verify that the Trend Micro Security Server is properly installed.

To verify the installation:

- Look for the WFBS program shortcuts on the Windows **Start** menu of the Trend Micro Security Server.
- Check if WFBS is in the **Add/Remove Programs** list.
- Log on to the Web console with the server's URL:

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

  If you are NOT using 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**

This Agent is installed on any of the following Trend Micro security solutions:

- WFBS: versions 5.0, 5.1, or 6.0
- Client/Server Messaging Security: versions 3.5 or 3.6

The following are also required:

- 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`.

   The following is an example:

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

2. Click **Yes** to signify 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**.
   c. Enter the customer information.
   d. Click **Next**.

   WARNING! If the customer already exists on the WFRM Console and you use the option above Associate with a new customer, this will result in two 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.
   c. Click **Next**.
5. 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 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 install 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). Client/Server Security Agents and Messaging Security Agents will upgrade automatically. See *Agent Installation Overview* on page 3-2.

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

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.

Supported Upgrades

WFBS 6.0 supports upgrades from any of the following versions:

- Client Server Security or Client Server Messaging Security 3.6
- Upgrade from Worry-Free Business Security or Worry-Free Business Security Advanced 5.0 and 5.1

Unsupported Upgrades

WFBS 6.0 does not support upgrades under the following conditions:

- Upgrade from Client/Server Messaging Security 3.5

- 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 Client/Server Security 3.0
- Upgrade from Client/Server/Messaging Security 3.0
- 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 different directory 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. 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 be given a Registration Key or an Activation Code.

To upgrade from an evaluation version:

1. Open the Web console.
2. On the main menu, click **Preferences** > **Product License**. The **Product License** screen appears.
3. Click **View license upgrade instructions**.
4. If you have an Activation Code, select **Enter a new code**, type it in the **New Activation Code** field, and click **Activate**.

Note: If you do not have an Activation Code, click **Register Online** and use the Registration Key to obtain an Activation Code.

Migrating from Other Antivirus Applications

WFBS supports migration from other antivirus applications. WFBS can automatically migrate the client software, but cannot uninstall the server application.

Migrating from Trend Micro Anti-Spyware

If you have Trend Micro Anti-Spyware on the network, take note of the following:

- If you install the Security Server on the same server as the TMASY server, the setup program will *not* remove or upgrade the TMASY server. You need to manually remove the TMASY server before installing the Security Server on the same machine.
- Removing the TMASY client before installing the Client/Server Security Agent is not required. The Client/Server Security Agent setup program will automatically remove the TMASY client when detected on the same client computer and then install Client/Server Security Agent.
- The anti-spyware settings for Client/Server Security Agent and TMASY are different. After installing the Client/Server Security Agents, you may need to configure the anti-spyware settings to make them the same as your previous TMASY client settings. Refer to *Table 4-2* for a comparison of the Client/Server Security Agent and TMASY anti-spyware settings.

TABLE 4-2. Comparison of Client/Server Security Agent and TMASY Anti-Spyware Settings

	CLIENT/SERVER SECURITY AGENT	TREND MICRO ANTI-SPYWARE CLIENT
Real-time Scan	Enabled	Disabled (Active Application Monitoring)
Default action	Clean	Deny executable
Manual Scan		
Scan type	Full scan	Quick scan
Default action	Clean	Scan and do nothing (auto clean is disabled by default)
Scan on start	N/A	Enabled
Check network	N/A	Enabled
Scheduled Scan	Disabled	Enabled
Scan schedule	Every Monday	Daily
Scan time	12:30	23:00
Scan type	Full scan	Quick scan
Default action	Clean	Scan and do nothing (auto clean is disabled by default)

Migrating from Other Antivirus Applications

Migrating from other 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 Client/Server Security Agent program. The client setup program automatically removes the other antivirus software on your client computers and replaces it with the Client/Server Security Agent.

Refer to *Table 4-3* for a list of client applications that WFBS can automatically remove.

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

TABLE 4-3. Removable Antivirus Applications

Trend Micro™		
Trend Micro™ OfficeScan 95 client 3.5 Trend Micro OfficeScan NT client version 3.1x Trend Micro OfficeScan NT client version 3.5 Trend Micro PC-cillin™ Corp 95 client PC-cillin Corp NT client Trend Micro ServerProtect™ for Windows NT Trend Micro™ PC-cillin 2004 (AV) Trend Micro PC-cillin 2004 (TIS) Trend Micro PC-cillin 2000 7.61(WinNT) Trend Micro PC-cillin 2000(Win9X)	Trend Micro PC-cillin 2000 for Windows NT Trend Micro PC-cillin 2002 Trend Micro PC-cillin 2003 Trend Micro PC-cillin 6 Trend Micro PC-cillin 95 1.0 Trend Micro PC-cillin 95 1.0 Lite Trend Micro PC-cillin 97 2.0 Trend Micro PC-cillin 97 3.0 Trend Micro PC-cillin 98 Trend Micro PC-cillin 98 Plus Windows 95 Trend Micro PC-cillin 98 Plus Windows NT Trend Micro PC-cillin NT Trend Micro PC-cillin NT 6 Trend Micro™ Virus Buster 2000	Trend Micro Virus Buster 2000 for NT ver.1.00 Trend Micro Virus Buster 2000 for NT ver.1.20 Trend Micro Virus Buster 2001 Trend Micro Virus Buster 98 Trend Micro Virus Buster 98 for NT Trend Micro Virus Buster NT Trend Micro Virus Buster 95 1.0 Trend Micro Virus Buster 97 Trend Micro Virus Buster 97 LiteOfficeScan 95 client 3.1x Trend Micro Virus Buster Lite 1.0 Trend Micro Virus Buster Lite 2.0

TABLE 4-3. Removable Antivirus Applications (Continued)

Symantec™		
Norton AntiVirus™ 2.0 NT	Norton AntiVirus 6.524	Norton Antivirus CE 8.0 9x
Norton AntiVirus 2000 9X	Norton AntiVirus 7.0 9X	Norton Antivirus CE 8.0 NT
Norton AntiVirus 2000 NT	Norton AntiVirus 7.0 NT	Norton Antivirus CE 8.1 server
Norton AntiVirus 2001 9X	Norton AntiVirus 7.5 9X	Norton Antivirus CE 9.0
Norton AntiVirus 2001 NT	Norton AntiVirus 7.5 NT	
Norton AntiVirus 2002 NT	Norton AntiVirus 8.0 9x	
Norton AntiVirus 2003	Norton AntiVirus 8.0 NT	
Norton AntiVirus 5.0 9X	Norton Antivirus CE 10.0	
Norton AntiVirus 5.0 NT	Norton Antivirus CE 10.1	
Norton AntiVirus 5.31 9X	Norton Antivirus CE 6.524	
Norton AntiVirus 5.31 NT	Norton Antivirus CE 7.0 for Windows NT	
Norton AntiVirus 5.32 9X	Norton Antivirus CE 7.0 NT	
Norton AntiVirus 5.32 NT	Norton Antivirus CE 7.5 9x	
	Norton Antivirus CE 7.5 NT	

TABLE 4-3. Removable Antivirus Applications (Continued)

McAfee™		
Dr Solomon 7.77,7.95 NT Dr Solomon 4.0.3 Dr Solomon 4.0.3 NT ePOAgent1000 ePOAgent2000 McAfee NetShield 4.5 McAfee NetShield NT 4.03a	McAfee VirusScan 4.5 McAfee VirusScan 4.51 McAfee VirusScan 6.01 McAfee VirusScan 95(1) McAfee VirusScan 95(2) McAfee VirusScan ASaP	McAfee VirusScan Enterprise 7 McAfee VirusScan NT McAfee VirusScan TC McAfee VirusScan(MSPlus98) V3Pro 98
LANDesk™		
LANDesk VirusProtect5.0		
Computer Associates™		
CA InocuLAN_NT 4.53 CA InocuLAN_9.x 4.53	CA eTrust InoculateIT 6.0	CA InocuLAN 5
Ahnlab™		
V3Pro 2000 Deluxe	V3Pro 98 Deluxe	
Panda Software™		
Panda Antivirus Local Networks	Panda Antivirus 6.0	Panda Antivirus Windows NT WS
F-Secure™		
F-Secure 4.04 F-Secure 4.08, 4.3 5.3	F-Secure BackWeb	F-Secure Management Agent
Kaspersky™		
Antivirus Personal 4.0, Workstation 3.5. 5.4		
Sophos™		
Sophos Anti-Virus NT	Sophos Anti-Virus 9X	
Authentium™		

TABLE 4-3. Removable Antivirus Applications (Continued)

Command AV 4.64 9x		
Amrein™		
Cheyenne AntiVirus 9X	Cheyenne AntiVirus NT	
Grisoft™		
Grisoft AVG 6.0		
Others		
ViRobot 2k Professional	Tegam ViGUARD 9.25e for Windows NT	

Upgrading the Client/Server 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, clients are automatically upgraded.

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 virus pattern file) 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.

The topics discussed in this chapter include:

Accessing the Web Console

This topic summarizes the Web console and how to access it.

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, 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.

When you install the Trend Micro Security Server, you also install the centralized Web-based management console. The console uses Internet technologies such as ActiveX, CGI, HTML, and HTTP/HTTPS.

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 in the **Password** text box, and then click **Log on**. The browser displays the **Live Status** screen of the Web console.

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 in 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**.

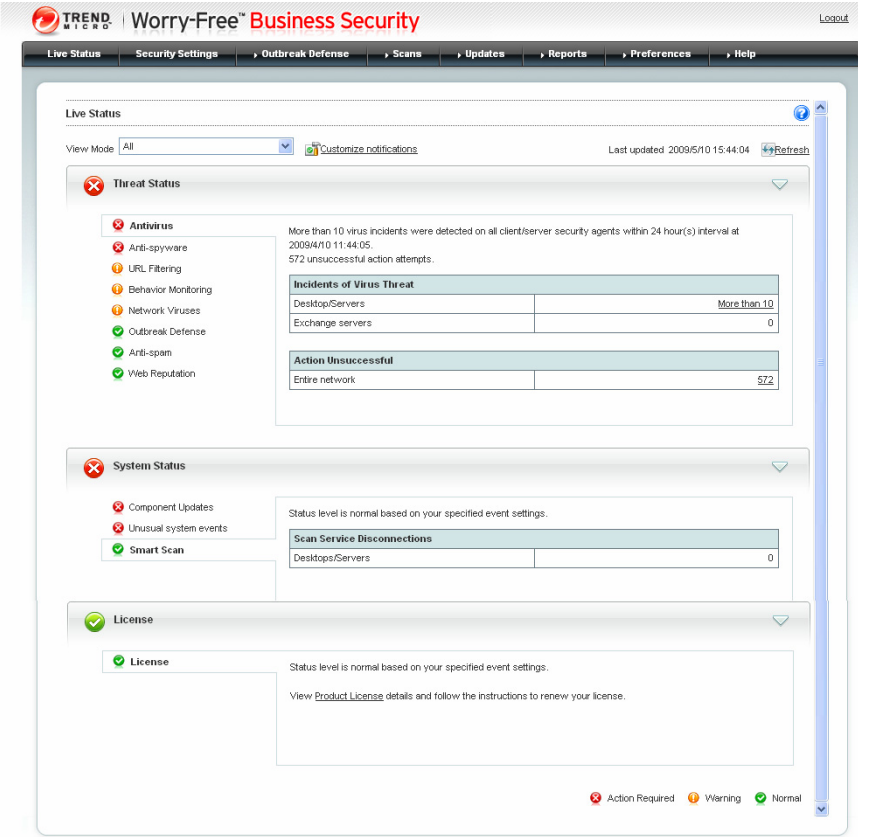

FIGURE 5-2. Live Status screen

Understanding Icons

Icons warn you if action is necessary to secure the computers on your network. 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

The Threat Status screen displays information about the following:

- **Antivirus:** virus detections. Starting from the 5th incident, the status icon changes to display the Warning. If you must take action:
  - The Client/Server 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 Client/Server Security Agent was unable to perform and take an action.
  - Real-time scanning is disabled on Client/Server Security Agents. Click **Enable Now** to start Real-time scanning again.
  - The real-time scanning is disabled on the Messaging Security Agent.
- **Anti-spyware:** The Anti-spyware section 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 Web sites as determined by the administrator. Starting from the 300th incident, the status icon changes to display the warning.
- **Behavior Monitoring:** violations of the behavior monitoring policies.
- **Network Viruses:** network virus detections determined by the firewall settings.
- **Outbreak Defense:** a possible virus outbreak on your network.
- **Anti-spam:** spam detections. 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 Web sites as determined by Trend Micro. Starting from the 200th incident, the status icon changes to display the warning.

System Status

View information regarding the updated components and the 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

View 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	CSA: Immediate MSA: 5
Anti-spyware	3	1
Anti-spam	3	60

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

Item	Update Interval (minutes)	Agent Sends Logs to Server After... (minutes)
Web Reputation	3	60
URL Filtering	3	60
Behavior Monitoring	3	60
Network Virus	3	60
Smart Scan	10	N/A
License	10	N/A
Component Updates	3	N/A
Unusual System Events	10	When the listening service TmListen is started

Viewing Security Settings

The Security Settings screen allows you to manage all the computers to which you installed the 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 remain available regardless of the options selected in the Security Settings screen are constant for all other screens.

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, Antivirus/Anti-spyware, Firewall, Web Reputation, URL Filtering, Behavior Monitoring, TrendSecure Toolbars, and Client Privileges, Mail Scan, and the Quarantine Directory for desktops and servers.

  Note: 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 Client/Server 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.

Chapter 6

Managing Basic Security Settings

This chapter explains how to configure settings to protect your network.

The 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, simultaneously configure and manage, multiple clients. For more information, refer to *Overview of 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	Switch between Smart Scan and Conventional Scan	Conventional Scan (for upgrade) Smart Scan (for new 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
Behavior Monitoring	Configure Behavior Monitoring options	Enabled for Desktop Groups Disabled for Server Groups
URL Filtering	URL filtering blocks Web sites that violate configured policies.	Enabled
TrendSecure	Configure In Office and Out of Office options for Transaction Protector and TrendProtect	In Office: Disabled Out of Office: Enabled
POP3 Mail Scan	Configure the scanning of POP3 email messages	Disabled

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

Option	Description	Default
Client Privileges	Configure access to settings from the client console	N/A
Quarantine	Specify the Quarantine directory	N/A

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

Scan Types

Virus scanning is a central part of the Worry-Free Business Security strategy. During a scan, the Trend Micro 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, the virus experts at TrendLabs 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 scan engine detects file containing a virus or other malware, it executes an action such as clean, quarantine, delete, or replace with text/file. You can customize these actions when you set up your scanning tasks.

WFBS provides three types of scans to protect clients from Internet threats:

- **Real-time Scan:** Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for threats.

  In the case of email messages, the Messaging Security Agent guards all known virus entry points with Real-time Scanning of all incoming messages, SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers.

- **Manual Scan:** Manual Scan is an on-demand scan. Manual Scanning eliminates threats from files. This scan also eradicates old infections, if any, to minimize reinfection. During a Manual Scan, agents take actions against threats according to the actions set by the Administrator (or User). To stop the scan, click **Stop Scanning** when the scan is in progress.

  Note: The time taken for the scan depends on the client's hardware resources and the number of files to be scanned.

- **Scheduled Scan:** A Scheduled Scan is similar to Manual Scan but scans all files and email messages at the configured time and frequency. Use Scheduled Scans to automate routine scans on your clients and improve the efficiency of threat management.

  To configure a Scheduled scan, click **Scans > Scheduled Scan**. Refer to *Scheduling Scans* for more information.

Note: Do not confuse the scan types above with scan methods. The scan method refers to Smart Scan and Conventional Scan (*Scan Methods* on page 7-2).

Configuring Real-time Scan

Navigation Path: Security Settings > Select a group > Configure > Antivirus/Anti-spyware

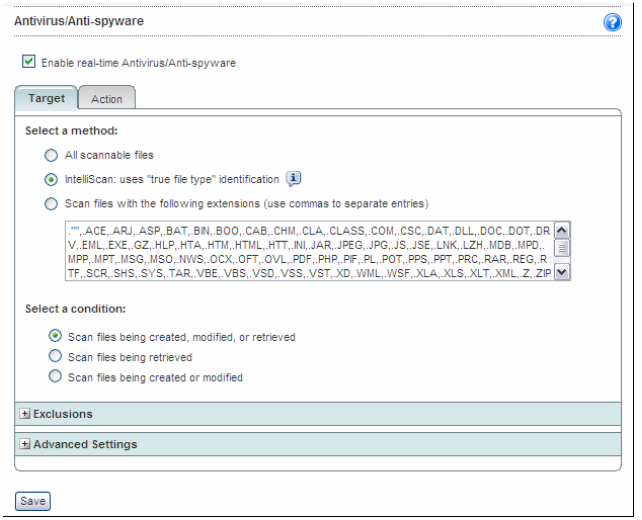

FIGURE 6-1. Security Settings > Antivirus/Anti-spyware screen

To configure Real-time Scan:

1. From the **Target** tab on the **Antivirus/Anti-spyware** screen, update the following as required:
   - **Enable real-time Antivirus/Anti-spyware**
   - **Files to scan**
     - **All scannable files:** Only encrypted or password-protected files are excluded.
     - **IntelliScan:** Scans files based on true-file type. Refer to *IntelliScan* on page C-4 for more information.

- **Scan files with the following extensions:** WFBS will scan files with the selected extensions. Separate multiple entries with commas (,).

- Select when to scan files
  - **Scan files being created, modified, or retrieved**
  - **Scan files being retrieved**
  - **Scan files being created or modified**
- **Exclusions:** Exclude specific files, folders, or files with certain extensions from being scanned.
  - **Enable Exclusions**
  - **Do not scan the directories where Trend Micro products are installed**
  - **Do not scan the following directories:** Type the name of the folder to exclude from the scan. Click **Add.** To remove a folder, select the folder and click **Delete**.
  - **Do not scan the following files:** Type the name of the file to exclude from the scan. Click **Add**. To remove a file, select the file and click **Delete**.
  - **Do not scan files with the following extensions:** Type the name of the extension to exclude from the scan. Click **Add.** To remove an extension, select the extension and click **Delete**.

Note: If Microsoft Exchange Server is running on the client, Trend Micro recommends excluding all Microsoft Exchange Server folders from scanning. To exclude scanning of Microsoft Exchange server folders on a global basis, go to **Preferences > Global Settings**, click the **Desktop/Server** tab, and then select **Exclude Microsoft Exchange server folders when installed on Microsoft Exchange server**.

- **Advanced Settings**
  - **Enable IntelliTrap** (for antivirus)**:** IntelliTrap detects malicious code such as bots in compressed files. Refer to *IntelliTrap* on page C-6 for more information.
  - **Scan mapped drives and shared folders on the network** (for antivirus)
  - **Scan floppy during system shutdown** (for antivirus)

- **Scan compressed files** (for antivirus)**:** Select the number of layers to scan.
- **Spyware/Grayware Approved List** (for anti-spyware)**:** This list contains details of the approved spyware/grayware applications. Click the link to update the list. Refer to *Editing the Spyware/Grayware Approved List* on page 7-7 for more information.

2. From the **Action** tab on the **Antivirus/Anti-spyware** screen, specify how WFBS should handle detected threats:
   - **Action for Virus Detections**
     - **ActiveAction:** Use Trend Micro preconfigured actions for threats. Refer to *ActiveAction* on page C-4 for more information.
     - **Perform the same action for all detected Internet threats:** Select from Pass, Delete, Rename, Quarantine, or Clean. If you select Clean, set the action for an uncleanable threat.
     - **Customized action for the following detected threats:** Select from Pass, Delete, Rename, Quarantine, or Clean for each type of threat. If you select Clean, set the action for an uncleanable threat.
     - **Backup detected file before cleaning:** Saves an encrypted copy of the infected file in the following directory on the client:

       ```
       C:\Program Files\Trend Micro\Client Server Security Agent\Backup
       ```
   - **Action for Spyware/Grayware Detections**
     - **Clean:** When cleaning spyware/grayware, WFBS could delete related registry entries, files, cookies, and shortcuts. Processes related to the spyware/grayware could also be terminated.
     - **Deny Access**

     WARNING! Denying spyware/grayware access to the client does not remove the spyware/grayware threat from infected clients.

   - **Advanced Settings**
     - **Display an alert message on the desktop or server when a virus/spyware is detected**

3. Click **Save.**

   Additionally, configure who receives notifications when an event occurs. Refer to *Configuring Events for Notifications* on page 8-3.

Managing the Firewall

Help protect clients from hacker attacks and network viruses by creating a barrier between the client and the network. Firewall can block or allow certain types of network traffic. Additionally, 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 Firewall.

Default Firewall Simple Mode Settings

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

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.

Intrusion Detection System

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.

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. Refer to *Location Awareness* on page 9-6.

Navigation Path: Security Settings > Select a group > Configure > Firewall > In Office/Out of Office

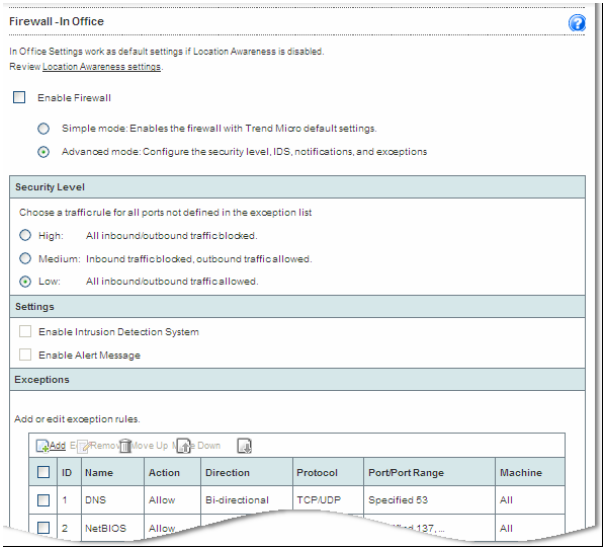

FIGURE 6-2. Firewall - In Office screen

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. Refer to *Default Firewall Settings* on page 6-9.
     - **Advanced Mode:** Enables firewall with custom settings. Refer to *Advanced Firewall Options* on page 6-13 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 inbound and outbound traffic.
     - **Medium:** Blocks inbound traffic and allows outbound.
     - **Low:** Allows inbound and outbound traffic.
   - Settings
     - **Enable Intrusion Detection System:** Intrusion Detection System identifies patterns in network packets that may indicate an attack. Refer to *Intrusion Detection System* on page 6-10 for more information.
     - **Enable Alert Messages:** When WFBS detects a violation, the client is notified.
   - **Exceptions:** Ports in the exception list will not be blocked. Refer to *Working with Firewall Exceptions* on page 6-15 for more information.
3. Click **Save**.

Disabling the Firewall

Navigation Path: Security Settings > Select a 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.

Working with Firewall Exceptions

Exceptions comprise specific settings that allow or block different kinds of traffic based on Direction, Protocol, Port and Machines.

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 Exceptions

To add an exception:

1. From the **Firewall - Advanced Mode** screen in the **Exceptions** section, click **Add**.
2. Update the options as required:
   - **Name:** Specify a unique name for the exception.
   - **Action: Block** or **Allow** the traffic for the selected protocol, ports, and clients.
   - **Direction: Inbound** refers to traffic flowing from the Internet and into your network. **Outbound** refers to traffic flowing from your network and into the Internet.
   - **Protocol:** The network traffic protocol for this exclusion.
   - **Ports**
     - **All ports** (default)
     - **Range**
     - **Specified ports:** Separate individual entries with commas.
   - **Machine**
     - **All IP addresses** (default)
     - **IP range**
     - **Single IP:** The IP address of a particular client.
3. Click **Save.** The **Firewall Configuration** screen appears with the new exception in the exception list.

Editing Exceptions

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. Refer to *Adding Exceptions* on page 6-15 for more information.
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**.

Using Web Reputation

Web Reputation helps prevent access to URLs that pose potential security risks by checking any requested URL against the Trend Micro Web Security database. Depending on the location (In Office/Out of Office) of the client, configure a different level of security.

If Web Reputation blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list. For information on adding a URL to the Approved URL list, refer to *Web Reputation and Approved URLs* on page 9-8 for more details.

Configuring Web Reputation

Navigation Path: Security Settings > Select a group > Configure > Web Reputation > In Office/Out of Office

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: 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. Refer to *Location Awareness* on page 9-6.

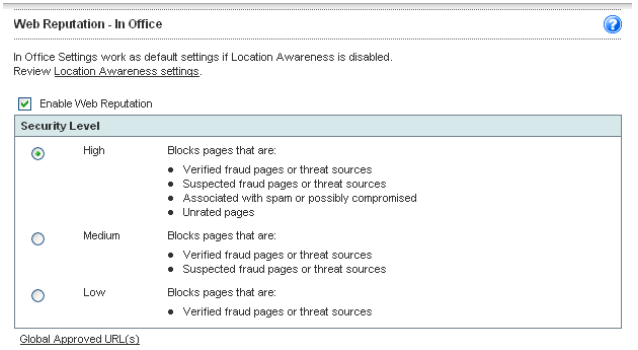

FIGURE 6-3. Security Settings > Web Reputation screen

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 verified fraud pages or threat sources, suspected fraud pages or threat sources, associated with spam or possibly compromised, unrated pages
     - **Medium:** Blocks pages that are verified fraud pages or threat sources, suspected fraud pages or threat sources
     - **Low:** Blocks pages that are verified fraud pages or threat sources

2. To modify the list of approved Web sites, click **Global Approved URL(s)** and modify your settings on the Global Settings screen.
3. Click **Save**.

Configuring URL Filtering

Navigation Path: Security Settings > Select Group > Configure > URL Filtering

Use URL filtering to block unwanted content from the Internet. You can select specific types of Web sites to block during different times of the day by selecting Custom. Also define Business Hours and Leisure Hours block Web sites during different times of the day.

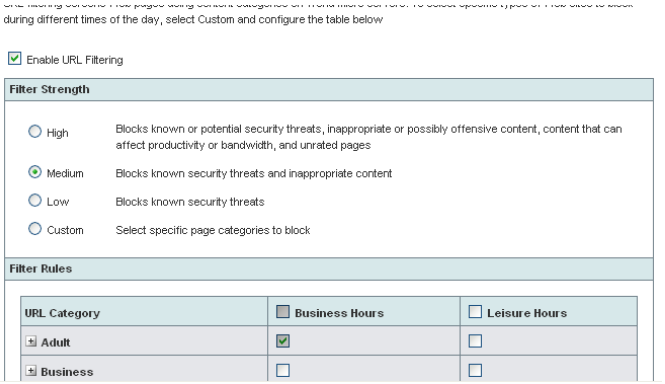

FIGURE 6-4. Security Settings > URL Filtering screen

To configure URL Filtering:

1. From the URL Filtering screen, update the following as required:
   - **Enable URL Filtering**

- **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.

2. Define your **Business Hours**.
3. To modify the list of approved Web Sites, click **Global Approved URL(s)** and modify your settings on the Global Settings screen.
4. Click **Save**.

Using 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.

Refer to the following table to view the description and default value of the monitored changes.

TABLE 6-3. Possible Changes Monitored

Monitored Change	Description	Default Value
Duplicated System File	Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.	Ask when necessary

TABLE 6-3. Possible Changes Monitored (Continued)

Monitored Change	Description	Default Value
Hosts File Modification	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the Web browser is redirected to infected, non-existent, or fake Web sites.	Always block
Suspicious Behavior	Suspicious behavior can be a specific action or a series of actions that is rarely carried out by legitimate programs. Programs exhibiting suspicious behavior should be used with caution.	Ask when necessary
System File Modification	Certain Windows system files determine system behavior, including startup programs and screen saver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.	Always block
New Internet Explorer Plugin	Spyware/grayware programs often install unwanted Internet Explorer plugins, including toolbars and Browser Helper Objects.	Ask when necessary
Internet Explorer Setting Modification	Many virus/malware change Internet Explorer settings, including the home page, trusted Web sites, proxy server settings, and menu extensions.	Always block
Security Policy Modification	Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.	Always block
Firewall Policy Modification	The Windows Firewall policy determines the applications that have access to the network, the ports that are open for communication, and the IP addresses that can communicate with the computer. Many malicious programs modify the policy to allow themselves to access to the network and the Internet.	Ask when necessary

TABLE 6-3. Possible Changes Monitored (Continued)

Monitored Change	Description	Default Value
Program Library Injection	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.	Ask when necessary
Shell Modification	Many malicious programs modify Windows shell settings to associate themselves to certain file types. This routine allows malicious programs to launch automatically if users open the associated files in Windows Explorer. Changes to Windows shell settings can also allow malicious programs to track the programs used and start alongside legitimate applications.	Ask when necessary
New Service	Windows services are processes that have special functions and typically run continuously in the background with full administrative access. Malicious programs sometimes install themselves as services to stay hidden.	Ask when necessary
System Process Modification	Many malicious programs perform various actions on built-in Windows processes. These actions can include terminating or modifying running processes.	Ask when necessary
New Startup Program	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.	Ask when necessary

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.

Configuring Behavior Monitoring

Navigation Path: Security Settings > Select a group > Configure > Behavior Monitoring

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

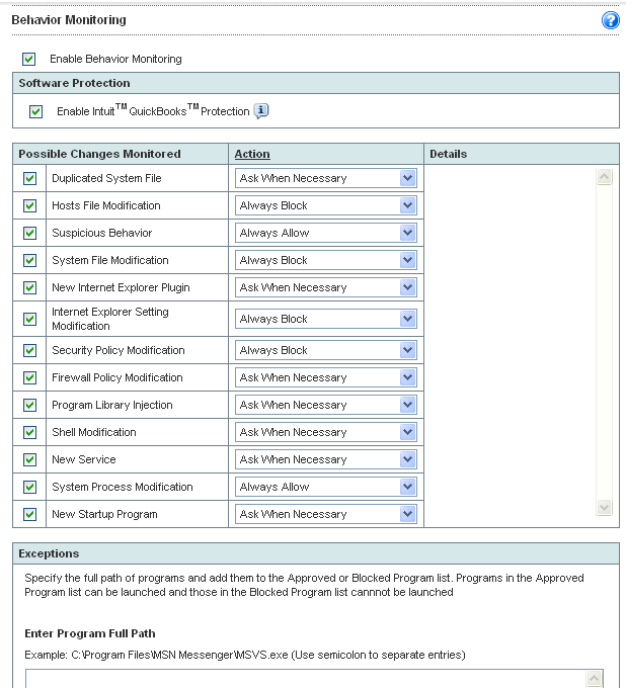

FIGURE 6-5. Behavior Monitoring screen

To edit Behavior Monitoring settings:

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

     Note: Navigate to **Security Settings > Select a group > Configure > Client Privileges** and select **Edit exception list** in the **Behavior Monitoring section**.

   - **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
   - **Prevent applications in USB plug-in devices from automatically opening:** Select this option to stop programs on USB devices from running automatically on clients.
   - **Possible Changes Monitored:** Select **Always Allow**, **Ask When Necessary**, or **Always Block** for each monitored change. Refer to Table 6-3 on page 6-19 for information on the different changes.
   - **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.
     - **Full Path of Program:** Type the full Windows or UNC path of the program. Separate multiple entries with semicolons (;). Click **Add to Approved Programs List** or **Add to Blocked Programs List**. Use environment variables to specify paths, if required. Refer to *Table 6-4* on page 6-24 for the list of supported variables.
     - **Approved Programs List:** Programs (maximum of 100) in this list can be started. Click the corresponding  icon to delete an entry.

- **Blocked Programs 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 6-4. Supported Variables

Environment Variable	Points to the...
$windir$	Windows folder
$rootdir$	root folder
$tempdir$	Windows temporary folder
$programdir$	Program Files folder

TrendSecure

TrendSecure comprises a set of browser-based tools (TrendProtect and Transaction Protector) that enable users to surf the Web securely. TrendProtect warns users about malicious and Phishing Web sites. Transaction Protector determines the safety of your wireless connection by checking the authenticity of the access point.

TrendSecure adds a browser toolbar that changes color depending on the safety of your wireless connection. You can also click the toolbar button to access the following features:

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

- **Page Ratings:** Determines the safety of the current page.

Note: Configure the TrendSecure settings for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. Refer to *Location Awareness* on page 9-6.

Configuring TrendSecure

Navigation Path: Security Settings > Select a group > Configure > TrendSecure Toolbars > In Office/Out of Office

Configure the availability of TrendSecure tools to users depending on their location.

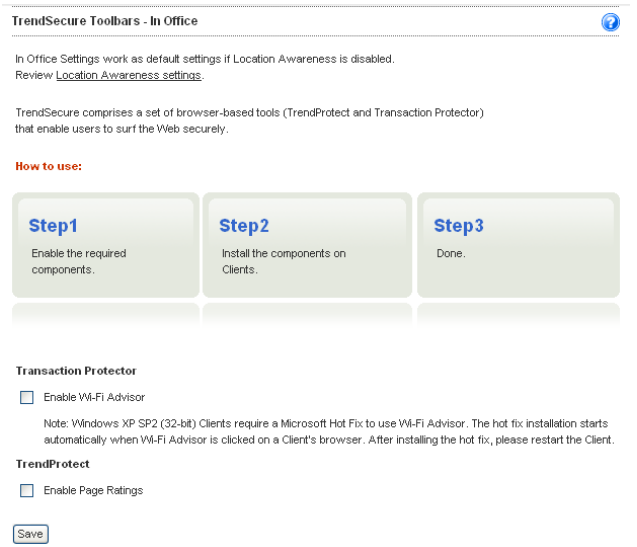

FIGURE 6-6. TrendSecure Toolbars - In Office screen

To edit the availability of TrendSecure tools:

1. From the **TrendSecure In Office/Out of Office** 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.
2. Click **Save.**

Note: TrendSecure 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.

Managing POP3 Mail Scan

POP3 Mail Scan and the Trend Micro Anti-Spam toolbar plug-in protect clients in real-time against security risks and spam transmitted through POP3 email messages.

Note: By default, POP3 Mail Scan can only scan new messages sent through port 110 in the Inbox and Junk Mail folders. It does not support secure POP3 (SSL-POP3), which is used by Exchange Server 2007 by default.

POP3 Mail Scan Requirements

POP3 Mail Scan supports the following mail clients:

- Microsoft Outlook™ 2000, 2002 (XP), 2003, and 2007
- Outlook Express™ 6.0 with Service Pack 2 (on Windows XP only)
- Windows Mail™ (on Microsoft Vista only)
- Mozilla Thunderbird 1.5 and 2.0

Note: POP3 Mail Scan cannot detect security risks and spam in IMAP messages. Use Messaging Security Agent to detect security risks and spam in IMAP messages.

Anti-Spam Toolbar Requirements

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

- Microsoft Outlook 2000, 2002 (XP), 2003, and 2007
- 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

Configuring Mail Scan

Navigation Path: Security Settings > Select a group > Configure > Mail Scan

To edit the availability of Mail Scan:

1. From the **Mail Scan** screen, update the following as required:
   - **Enable real-time scan for POP3 mail**
   - **Enable Trend Micro Anti-Spam toolbar**
2. Click **Save**.

Client Privileges

Navigation Path: Security Settings > Select a 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 Client/Server Security Agent.

Configuring Client Privileges

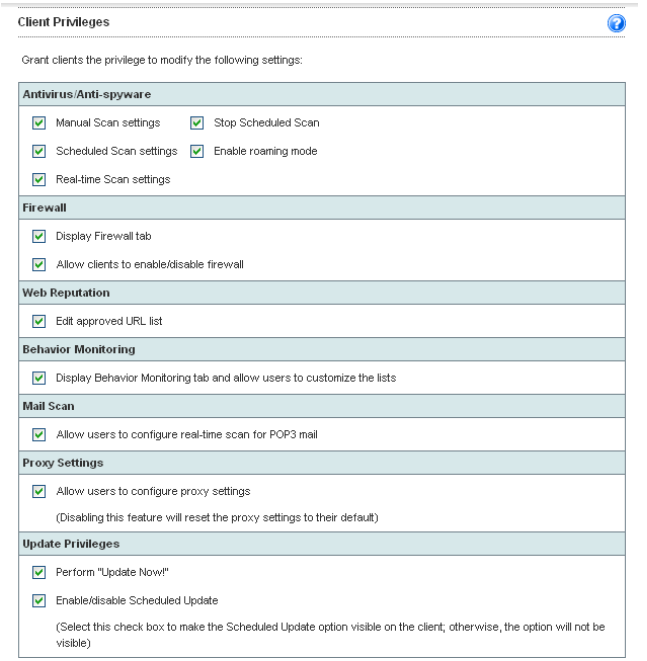

FIGURE 6-7. Client Privileges screen

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**
     - **Stop Scheduled Scan**
     - **Enable roaming mode**
   - **Firewall**
     - **Display Firewall tab**
     - **Allow clients to enable/disable firewall**

     Note: If you allow users to enable or disable the firewall, you cannot change these settings from the Web console. If you do not grant users this privilege, you can change these settings from the Web console. The information under **Local Firewall settings** on the agent always reflects the settings configured from the agent, not the Web console.

   - **Web Reputation**
     - **Edit approved URL list**
   - **Behavior Monitoring**
     - **Display Behavior Monitoring tab and allow users to customize the lists:** Allow users to enable/disable Behavior Monitoring and configure the Exception List and the Software Protection List.
   - **Mail Scan**
     - **Allow users to configure real-time scan for POP3 mail**
   - **Proxy Settings**
     - **Allow users to configure proxy settings**
   - **Update Privileges**
     - **Perform "Update Now"**
     - **Enable/Disable Scheduled Update**
   - **Update Settings**

- **Download from Trend Micro ActiveUpdate Server:** When users initiate an update, the agent gets updates from the update source specified on the **Update Source** screen. If the update fails, the agents attempt to update from the Security Server. Selecting **Download from the Trend Micro ActiveUpdate Server** enables agents to attempt to update from the Trend Micro ActiveUpdate Server if the update from the Security Server fails.

Tip: To ensure agents on portable clients are updated when they are out of the office, enable **Download from Trend Micro ActiveUpdate Server.**

- **Enable Scheduled Update**
- **Disable program upgrade and hot fix deployment**

- **Client Security**
  - **High**
    - Denies write access to client registry keys and the client installation folder
    - Prevents client processes and services from being stopped
  - **Normal:** Allows read/write access to agent folders, files, and registry entries.

Note: If you select **High**, the access permissions settings of the agent folders, files, and registry entries are inherited from the Program Files folder (for clients running Windows Vista/2000/XP/Server 2003).
Therefore, if the permissions settings (security settings in Windows) of the Windows file or Program Files folder are set to allow full read/write access, selecting **High** still allows clients full read/write access to the Client/Server Security Agent folders, files, and registry entries.

---

2. Click **Save**.

Managing the Quarantine

The quarantine directory stores infected files. The quarantine directory can reside on the client itself or on another server. If an invalid quarantine directory is specified, agents use the default quarantine directory on the client:

```
C:\Program Files\Trend Micro\Client Server Security
Agent\SUSPECT
```

The default folder on the server is:

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

Note: If the CSA 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 > Select a group > Configure > Quarantine

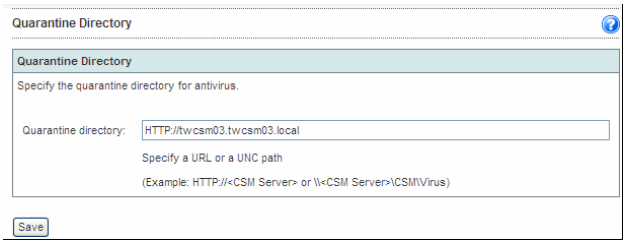

FIGURE 6-8. Quarantine Directory screen

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 3-8).
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

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

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

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

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. Refer to 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 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 Client/Server Security Agent uses the third-party software's uninstallation program to automatically remove it from your users' system and replace it with the Client/Server 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

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**.

   For Windows 2000, also do the following:

5. Go to

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TRENDMICRO\ScanMail for Microsoft Exchange
   ```

6. Click **ScanMail for Microsoft Exchange**.

7. Select **Security > Permissions**.
8. Add **Smex Admin Group** of target domain, and enable **Allow Read** and **Allow Full Control**.

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 Web site.

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 Web site 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?

Refer to the WFBS *Installation Guide* for information.

Which Agent installation method is best for my network environment?

Refer to *Agent Installation Overview* 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 Client/Server 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. Contact Support if you lost or forgot your password.

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?

Refer to the following tables for the SBS 2003 exclusions:

TABLE A-1. Microsoft Exchange Exclusions

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 9-7 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 Web site:

  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 Web site is subject to change without notice.

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 Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

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

Visit the Security Information site 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 Virus 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

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 Web site and receive the Activation Code(s).
ActiveUpdate	Connected to the Trend Micro update Web site, 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.
Administrator	A type of virus that resides in Web pages that execute ActiveX controls.
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 Client/Server Security Agent is installed.
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.
Conventional Scan	A local scan engine on the client scans the client computer.

Term	Description
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.
Live Status	The main screen or dashboard of the Web Console. Live Status gives you an at-a-glance security status for Outbreak Defense, Antivirus, Anti-spyware, and Network Viruses.
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.
privileges (client privileges)	From the Web console, Administrators can set privileges for the Client/Server Security Agents. End users can then set the Client/Server 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.

Term	Description
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 Client/Server 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.
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.
TrendSecure	TrendSecure comprises a set of browser-based plugin tools (TrendProtect and Transaction Protector) that enable users to surf the Web securely. TrendProtect warns users about malicious and Phishing Web sites. Transaction Protector determines the safety of your wireless connection by checking the authenticity of the access point.
Update Agent	Agents that act as update sources for other agents.
Web console	The Web console is a centralized Web-based management console. You can use it to configure the settings of Client/Server 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.

Index

Q

R

S

T

U

V

W