Worry-Free™ Business Security Services

for Small and Medium Business

Safer. Smarter. Simpler.

User's Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Release Date: April 2011

Product Name and Version No.: Trend Micro™ Worry-Free™ Business Security Services 3.5 SP3

Document Version No: 1.02

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

The user documentation for Trend Micro™ Worry-Free™ Business Security Services 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 Worry-Free™ Business Security Services

Chapter 2: Preparing for Agent Installation

Chapter 3: Agent Installation

Chapter 4: Migrating and Upgrading

Chapter 5: Web Console

Chapter 6: Managing Groups

Chapter 7: Configuring Group Security Settings

Chapter 8: Managing Scans

Chapter 9: Using Outbreak Defense

Chapter 10: Managing Notifications

Chapter 11: Configuring Global Settings

Chapter 12: Managing Updates

Chapter 13: Using Logs and Reports

Chapter 14: Administering WFBS-SVC

Appendix A: Client Information

Appendix B: Trend Micro Services

Appendix C: Best Practices for Protecting Your Clients

Appendix D: Troubleshooting and Frequently Asked Questions

Appendix E: Getting Help

Appendix F: Glossary

Index

Chapter 1

Introducing Worry-Free™ Business Security Services

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

The topics discussed in this chapter include:

Overview of Trend Micro™ Worry-Free™ Business Security Services

Trend Micro™ Worry-Free™ Business Security Services for small offices protects multiple PCs and notebooks located in or out of the office from viruses and other threats from the Web. Unique Web Threat Protection stops threats before they reach computers and inflict damage or steal data. This safer, smarter, simpler protection from Web threats won't cause computers to slow down. You can centrally manage security from anywhere without the need to add a server, install server software, configure settings, or maintain updates. Trend Micro security experts host and constantly update the service for you. Trend Micro™ Worry-Free™ Business Security Services is:

- **Safer:** Protect multiple PCs/notebooks located in or out of the office with a single antivirus, anti-spyware business solution.
- **Smarter:** Stop viruses and other threats without configuring settings or maintaining updates.
- **Simpler:** Centrally manage and check the status of protected computers anywhere (no server required).

WFBS, WFBS-A, WFBS-SVC

The following table lists the features supported for each edition.

TABLE 1-1. Features Available by Product Editions

FEATURES	WORRY-FREE BUSINESS SECURITY	WORRY-FREE BUSINESS SECURITY ADVANCED	WORRY-FREE BUSINESS SECURITY SERVICES
Component Updates	Yes	Yes	Yes
Antivirus/Anti-spyware	Yes	Yes	Yes
Firewall	Yes	Yes	Yes
Web Reputation	Yes	Yes	Yes
Behavior Monitoring	Yes	Yes	Yes
TrendSecure	Yes	Yes	Yes
Instant Messaging Content Filtering	Yes	Yes	Yes
Mail Scan (POP3)	Yes	Yes	Yes
Anti-Spam (POP3)	Yes	Yes	Yes
Mail Scan (IMAP)	No	Yes	No
Anti-Spam (IMAP)	No	Yes	No
Email Message Content Filtering	No	Yes	No
Attachment Blocking	No	Yes	No
URL Filtering	Yes	Yes	Yes
Server Required	Yes	Yes	No

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

TABLE 1-2. License Status Consequences

	FULLY LICENSED	TRIAL (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 sales representative.

Choosing Your Edition

Full Version and Trial Version

You can choose either a full version of WFBS-SVC or a free, trial version.

- **Full version:** Comes with technical support, virus pattern downloads, real-time scanning, and program updates. You can renew a full version by purchasing a maintenance renewal.
- **Trial version:** Provides real-time scanning and updates for 30 days. You can upgrade from an trial version to a full version at any time.

Grace Periods

If you allow your license to expire, you will have a grace period of 30 days for the full version. During the grace period, you can still receive new pattern and engine updates and all features will still function normally. After the grace period ends, you will no longer be able to log on.

For a full license, 30 days after the grace period, all customer data will be deleted from the WFBS-SVC system. For a trial license, all customer data will be deleted 30 days after the trial ends.

What's New in This Release?

Version 3.5 SP3

- URL Block list for URL Filtering
- Wildcards allowed in URL Block and Allow lists for URL Filtering
- An add-in tool will allow administrators to access the WFBS-SVC console directly from a Small Business Server (SBS) Essentials 2011 Dashboard
- Support for Microsoft Internet Explorer 9

Version 3.5

- **URL 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 *URL Filtering* on page 7-9 for more information.
- Administrators can now set a password to avoid unauthorized uninstallation or shutdown of the Agent. See *Agent Uninstallation* on page 11-6 and *Agent Shut Down (Unload)* on page 11-6 for more information.
- URL filtering information now available in the logs. See *Logs* on page 13-5 for more information.

Version 3.0

Worry-Free Business Security Hosted (WFBS-H) has been renamed to Worry-Free Business Security Services (WFBS-SVC).

WFBS-SVC has an entirely new interface with a greatly expanded feature set over that of WFBS-H. WFBS-SVC includes most of the features of WFBS 6.0.

The following are new in this release of Trend Micro™ Worry-Free™ Business Security Services:

Security

- Smart Scan
- Smart Protection Network Integration
- Protection from USB autorun threats
- Outbreak Prevention
- Behavior Monitoring

Management

- Simpler and easier Live Status
- Live Status Notification Enhancement
- Integration with Worry-Free™ Remote Manager

Others

- Variable Scanning based on CPU consumption
- Support for Windows™ 7

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, 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.

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

Protecting Your Network

WFBS-SVC protection consists of the following components:

- **The Web Console:** manages all agents from a single location.
- WFBS-SVC **Server:** hosts the Web console at a Trend Micro data center. It collects and stores logs and helps control virus/malware outbreaks.
- **Client/Server Security Agent:** a small program on the client machine that protects Windows Vista/Windows 7/2000/XP/Server 2003/Server 2008 computers from virus/malware, spyware/grayware, Trojans, and other threats.
- **Scan Server:** enables scanning of clients via server-held pattern files, reducing the overall load on the client.

The Web Console

The Web console is a centralized, Web-based, management console located at Trend Micro data centers. Use the Web console to configure your protection environment.

Also use the Web console to:

- 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 when threats are detected on clients.
- Control outbreaks by enabling Outbreak Prevention.

WFBS-SVC Server

At the center of WFBS-SVC is the Server. The Server hosts the centralized Web-based management console for WFBS-SVC. The Server, along with the Agents, forms a client-server relationship. The WFBS-SVC Server enables viewing security status information, viewing Agents, configuring system security, and updating Agent components from a centralized location. The Server also contains the database where it stores logs of detected Internet threats being reported to it by the Agents.

Client/Server Security Agent

The Client/Server Security Agent reports to the WFBS-SVC Server. 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.

Agent scan settings can be configured from either the Web console or on the Agent itself. To enforce uniform desktop protection across the network, do not grant users privileges to modify the scan settings.

Scan Server

As part of the Smart Protection Network, WFBS-SVC provides the ability to scan your clients with a Scan Server. The Scan Server takes the burden of scanning computers off your clients and puts it on a scan server.

Scan Engine

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

- Actively circulating: Threats that are actively circulating on the Internet
- Known and controlled: Controlled viruses not in circulation, but that are developed and used for research

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

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

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

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

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

Scan Engine Updates

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

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

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

http://www.trendmicro.com

Benefits of Protection

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

TABLE 1-3. **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

TABLE 1-3. Benefits of Protection

THREAT	PROTECTION
Virus/Malware and Spyware/Grayware transmitted through email messages and spam	POP3 Mail Scan in Client/Server Security Agent
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 Agents:** 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 Client/Server 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.

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-SVC 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, the 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 WFBS-SVC Console 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.

Live Status and Notifications

- Live Status gives you an at-a-glance security status for Outbreak Defense, Antivirus, Anti-spyware, and Network Viruses. WFBS-SVC 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, 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.

Certain applications are classified by Trend Micro as spyware/grayware not because they can cause harm to the system on which they are installed, but because they potentially, expose the Client or the network to malware or hacker attacks.

Hotbar, for example, is a program that embeds a toolbar into Web browsers. Hotbar tracks URLs that users visit and records words or phrases that are entered into search engines. These pieces of information are used to display targeted ads, including pop-ups, on users' browsers. Since the information that Hotbar collects can potentially sent to a third party site and used by malware or hackers to collect information about your users, Worry-Free Business Security Services prevents this application from installing and running by default.

If you want to run Hotbar or any other application that WFBS-SVC classifies as spyware/grayware, you need to add it to the spyware/grayware trusted list.

By preventing potentially risky applications from running and giving you full control over the spyware/grayware trusted list, WFBS-SVC helps ensure that only the applications you approve run on Clients.

Client/Server 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.

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 1-10 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*.

Product Component Terminology

The following table defines the terms that appear in WFBS-SVC documentation:

TABLE 1-4. Product Component Terminology

ITEM	DESCRIPTION
WFBS-SVC Server	The WFBS-SVC Server at the Trend Micro Data Center hosts the Web console, the centralized Web-based management console for the entire WFBS-SVC solution.
Scan Server	The Trend Micro Global Scan Server helps scan clients that are configured for Smart Scan.
CSA	The Client/Server Security Agent. Agents protect the client it is installed on.
Client	Clients are desktops, portable computers, and servers where 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 WFBS-SVC Server.

Document Conventions

To help you locate and interpret information easily, the WFBS-SVC documentation uses the following conventions.

TABLE 1-5. Conventions and terms used in the document

CONVENTION/TERM	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation
`Monospace`	Sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip	Recommendations
WARNING!	Critical actions and configuration options
Navigation Path	The navigation path to reach a particular screen. For example, **Scans > Manual Scans**, means, click **Scans**, and then click **Manual Scans** on the interface.

Chapter 2

Preparing for Agent Installation

The steps in this chapter help you develop a plan for WFBS-SVC 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 section include:

- *Before You Begin* on page 2-2
- *System Requirements* on page 2-3
- *Registering WFBS-SVC* on page 2-5
- *License and Maintenance Agreement* on page 2-5
- *Deployment Checklist* on page 2-5
- *Ports Checklist* on page 2-7

Before You Begin

Review the following phases of installation and deployment.

Phase 1: Deployment Planning

Planning the WFBS-SVC deployment includes the following tasks:

1. Verifying system requirements. See *System Requirements* on page 2-3.
2. Identifying the number of clients. See *Identifying the Number of Clients* on page 2-6.
3. Planning for network traffic. See *Planning for Network Traffic* on page 2-6.
4. Determining desktop and server groups. See *Determining the Number of Desktop and Server Groups* on page 2-7.
5. Choosing installation/deployment options for Client/Server Security Agents. See *Choosing Deployment Options for Agents* on page 2-7.

Phase 2: Installing Agents

Install Client/Server Security Agent on all servers and desktops. This phase includes the following tasks:

Note: See *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 3: Configuring Security Options

After installing Client/Server Security Agent on Clients, customize the default settings if required. This includes the following tasks:

1. Configuring groups. See *Overview of Groups* on page 6-2
2. Configuring preferences. See *Configuring Desktop and Server Groups* on page 7-2

System Requirements

To install the Agent and use WFBS-SVC, the following is required:

Note: The Client/Server Security Agent supports Citrix Presentation Server™ 4.0/4.5/5.0 and Remote Desktop.

TABLE 2-6. **System Requirements**

Item	Minimum Specifications
Web Console	
Web browser	Internet Explorer 7.0 or later (32 and 64 bit) Firefox 3.5 and later (Firefox is only supported for the WFBS-SVC console. Internet Explorer must be used to download the Agent installer).
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 64 technologies Clock speed requirements vary depending on the operating system: • **SBS 2008, SBS 2011:** 2GHz • **Windows Server 2008, EBS 2008:** 1GHz • **Windows Vista, Windows 7:** 800MHz • **Windows 2000, SBS 2000, XP, Server 2003, SBS 2003, Home Server:** 450MHz
Memory	• **Windows SBS 2008, EBS 2008, SBS 2011:** 4GB • **Windows Server 2008, SBS 2000 or 2003:** 1GB minimum; 2GB recommended • **Windows 2000 Server, Server 2003, Home Server, Windows Vista, Windows 7**: 512MB minimum; 1GB recommended • **Windows 2000, Windows XP:** 256MB minimum; 512MB recommended
Disk space	600MB

TABLE 2-6. **System Requirements**

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 Home	SP2 or SP3
	Windows XP Tablet PC	SP2 or SP3
	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
	Windows Server 2008 R2	None or SP1
	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
	Windows 7	None or SP1
	Windows SBS 2011	No service pack
	Note: All major editions and 64-bit versions of these operating systems are supported unless noted otherwise.	
Web browser (for downloading Agent Installer)	Internet Explorer 7.0 or later	
Display	256-color display or higher with resolutions of 800x600 or higher	

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

Other Requirements

- Clients that use Smart Scan must be connected to the Internet. Offline clients cannot use Smart Scan.
- Transmission Control Protocol/Internet Protocol (TCP/IP) support installed

Registering WFBS-SVC

To register your product, follow the instructions on the relevant WFBS-SVC Quick Start Card which can be downloaded from

http://www.trendmicro.com/ftp/documentation/guides/WFBS-SVC_QSC_en.pdf

If you have questions about registration, consult the Trend Micro Web site at the following address: http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326.

You can also contact your reseller or Trend Micro support.

License and Maintenance Agreement

When you purchase Trend Micro™ Worry-Free™ Business Security Services, 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 sales representative.

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 trial 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.

Deployment Checklist

Look over the following before you deploy WFBS-SVC. Pay attention to the following two issues:

- **CSA and OneCare**

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

- **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-SVC firewall.

Identifying the Number of Clients

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

Planning for Network Traffic

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

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

Note: Other than updates and log generation, all the other actions generate a small amount of traffic.

Network Traffic During Pattern File Updates

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

To reduce network traffic generated during pattern file updates, WFBS-SVC uses a method called incremental update. Instead of downloading the full updated pattern file every time, new patterns that have been added since the last release are downloaded.

WFBS-SVC also uses Active and Inactive Agents. The Active Agent will update itself from the Trend Micro Active Update Server and so will generate Internet traffic. The Inactive Agents will update themselves from the Active Agent and so will generate internal network traffic.

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

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.

A WFBS-SVC 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.

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.

If you have a small office, you may only have one group.

Choosing Deployment Options for Agents

WFBS-SVC 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 a Login Script Setup. 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 Login Script Setup is recommended. 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 via simple Agent download is recommended. The administrator sends out an email message instructing users to visit the download site where they can install Client/Server Security Agent. Using this method, however, requires that end users who will install the Agent have administrator privileges.

For more information about the installation methods, see *Agent Installation Overview* on page 3-2

Ports Checklist

WFBS-SVC uses the following default ports.

TABLE 2-7. Port Checklist

PORT	DEFAULT	YOUR VALUE
Client/Server Security Agent	21112 (TCP)	
Agent HTTP server	61116 (TCP)	
Agent broadcast	61117 (UDP)	
Agent downloader	61119 (UDP)	

Chapter 3

Agent Installation

The Client/Server Security Agent reports to the WFBS-SVC Server. 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.

This chapter explains the steps necessary for installing, upgrading and removing Agents including:

- *Agent Installation Overview* on page 3-2
- *Agent Installation - Web* on page 3-2
- *Agent Installation - Additional Options* on page 3-6
- *Verifying Agent Installation* on page 3-8
- *Testing the Client Installation with the EICAR Test Script* on page 3-9
- *Removing Agents* on page 3-9

Agent Installation Overview

Navigation Path: Computers > Add > Computers

This section provides information on installing the Client/Server Security Agent. WFBS-SVC provides two categories of Agent Installation:

- **Web Installation:** Direct download and immediate installation of the Agent (see *Agent Installation - Web* on page 3-2)
- **Additional Installation Options:** Download the Agent installer (See *Agent Installation - Additional Options* on page 3-6) which can then be deployed via:
  - **Conventional installation:** Download and copy the installation file to client computers
  - **Windows startup script:** Allows for deployment of the Agent via Windows startup script--an advanced option useful for when there are a large number of Agents to be installed.

Note: To install the Client/Server Security Agent, you must have local Administrator rights on the clients.

Note: To prevent users from uninstalling Security Agents, require a password for uninstalling the Agent at **Preferences > Global Settings**. See *Agent Uninstallation* on page 11-6.

Agent Installation - Web

Navigation Path: Computers > Add > Add Computers

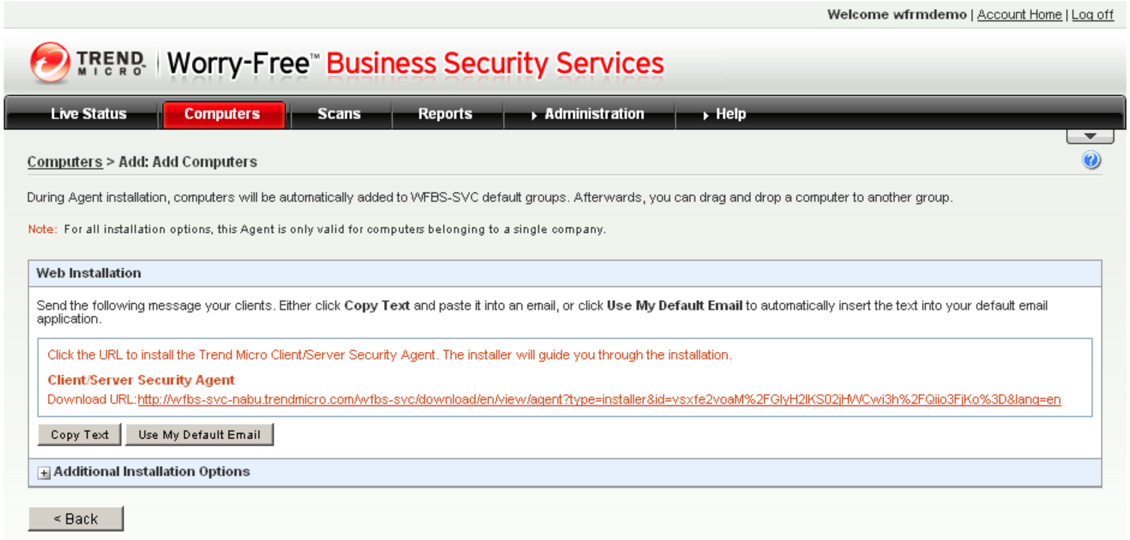
Web installation is a convenient way to deploy the Client/Server Security Agent. You only have to email the text (which includes the URL of the installation file) from the WFBS-SVC console to your users. Your clients can then download the Agent installation file and install the Agent.

Users must have Microsoft™ Internet Explorer™ 7.0 or later with the security level set to allow cookies to successfully download the Client/Server Security Agent installation files.

Note: The Agent uses the proxy settings in Internet Explorer under **Tools > Internet Options > Connections > LAN Settings** to access the Internet.

To distribute installation instructions to users:

1. On the WFBS-SVC console, go to **Computers > Add > Add Computers**.


Welcome wfrmdemo | Account Home | Log off
TREND MICRO
Worry-Free™ Business Security Services
Live Status
Computers
Scans
Reports
Administration
Help

Computers > Add: Add Computers

During Agent installation, computers will be automatically added to WFBS-SVC default groups. Afterwards, you can drag and drop a computer to another group.

Note: For all installation options, this Agent is only valid for computers belonging to a single company.

Web Installation

Send the following message your clients. Either click **Copy Text** and paste it into an email, or click **Use My Default Email** to automatically insert the text into your default email application.

Click the URL to install the Trend Micro Client/Server Security Agent. The installer will guide you through the installation.

Client/Server Security Agent

Download URL:http://wfbs-svc-nabu.trendmicro.com/wfbs-svc/download/en/view/agent?type=installer&id=vsxfe2voaM%2FGlyH2lKS02jHWCwi3h%2FQiio3FjKo%3D&lang=en

FIGURE 3-1. Send this message and URL to clients for a Web installation

Note: Each WFBS-SVC account is assigned a specific company key. The company key is a unique set of characters contained in a downloaded cookie. This key is then combined with the Agent during the installation process. The key links the Agent with the appropriate company account on the WFBS-SVC console. Because of this, the Agent installer cannot be copied from computer to computer. To obtain a copy of the Agent installer that can be copied from computer to computer, follow the instructions for other installation options (see *Agent Installation - Additional Options* on page 3-6).

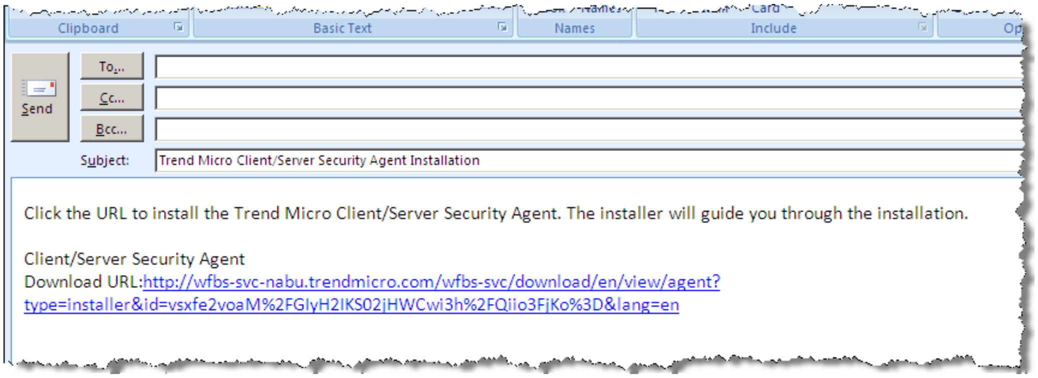
2. Click **Use My Default Email** to copy the download URL into your default email client to send to your users (or click **Copy Text** to copy the URL and then paste it into your email client).

WARNING! **If you are a reseller, you must log into each company that you are administering separately to either obtain the download URL for distribution via email or to download the Agent installer for conventional or scripted installation. If you install an Agent using the wrong URL or Agent installer, the Agent will show up under the wrong customer and will have to be reinstalled using the correct installer.**

The instructions below are written from the end user's perspective.

To install the Agent via Web installation:

1. Click the **Download** URL in the email.



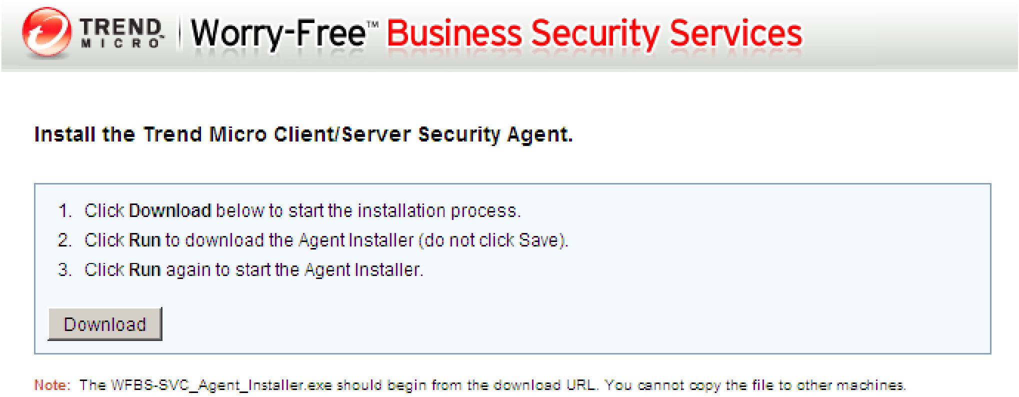
Subject: Trend Micro Client/Server Security Agent Installation

Click the URL to install the Trend Micro Client/Server Security Agent. The installer will guide you through the installation.

Client/Server Security Agent
Download URL:http://wfbs-svc-nabu.trendmicro.com/wfbs-svc/download/en/view/agent?type=installer&id=vsxfe2voaM%2FGlyH2IKS02jHWCwi3h%2FQiio3FjKo%3D&lang=en

FIGURE 3-2. Email the download URL to users

2. When the Web page opens, click **Download** to start the installation process.



Install the Trend Micro Client/Server Security Agent.

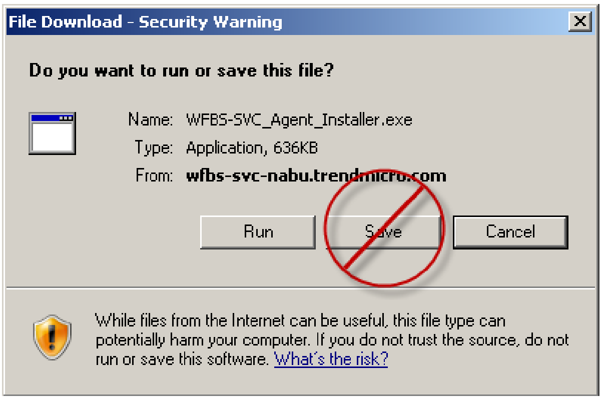
1. Click **Download** below to start the installation process.
2. Click **Run** to download the Agent Installer (do not click Save).
3. Click **Run** again to start the Agent Installer.

Note: The WFBS-SVC_Agent_Installer.exe should begin from the download URL. You cannot copy the file to other machines.

FIGURE 3-3. Click Download to start the Agent installation process

3. When the first security warning opens, click **Run**. Do not click Save.

   (This file cannot be copied to any other computer. To obtain a copy of the Agent installer that can be copied from computer to computer, see *Agent Installation - Additional Options* on page 3-6).



File Download - Security Warning

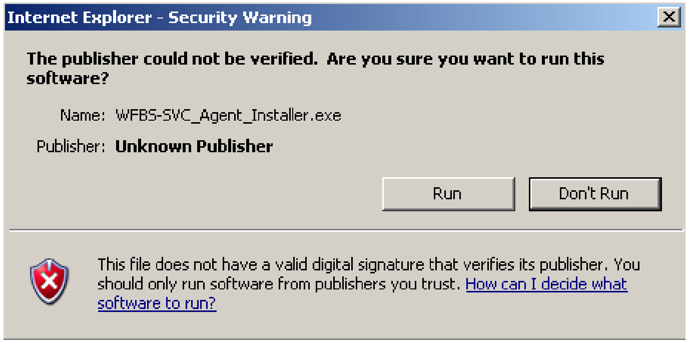
Do you want to run or save this file?

Name: WFBS-SVC_Agent_Installer.exe
Type: Application, 636KB
From: **wfbs-svc-nabu.trendmicro.com**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

FIGURE 3-4. Do not click Save on the first security warning. This file is not usable anywhere except for installation on the original, download computer.

4. When the second security warning opens, click **Run** again.



Internet Explorer - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: WFBS-SVC_Agent_Installer.exe
Publisher: **Unknown Publisher**

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

FIGURE 3-5. Click Run on the second security warning

5. The Agent installer will continue downloading (which can take a while). Once the Agent installer opens, click **Next** to begin installing the Client/Server Security Agent.

   The installation starts. Once installation is completed, the screen displays the message: **Installation Successful**.

6. Verify the installation by checking if the Client/Server Security Agent icon appears in the Windows system tray. It should be one of the following icons:

   - For Conventional Scan:
   - For Smart Scan:

Agent Installation - Additional Options

Navigation Path: Computers > Add > Add Computers

Additional Installation Options include:

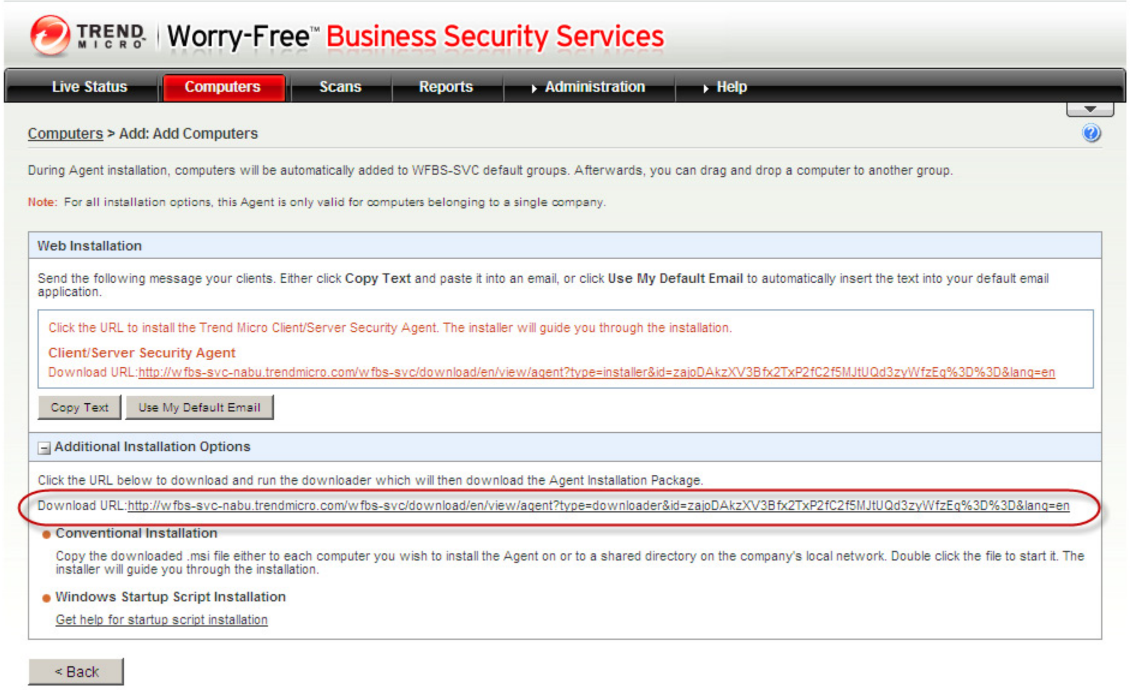
- **Conventional installation:** allows single file installation.
- **Windows startup script:** allows for deployment of the Agent via Windows startup script--a more efficient option useful for when there are a large number of Agents to be installed.

The download process first downloads `WFBS-SVC_Downloader.exe`. The downloader then downloads the Agent installer called `WFBS-SVC_Agent_Installer.msi` and a cookie containing the company key. The downloader then inserts the company key into the Agent installer so that the installer can be distributed.

WARNING! **The downloader (`WFBS-SVC_Downloader.exe`) cannot be distributed amongst client computers. Only `WFBS-SVC_Agent_Installer.msi` using the proper download procedure outlined in this section can be used for deploying Agents to other computers.**

To download the Agent installer:

1. On the WFBS-SVC console, go to **Computers > Add > Add Computers**.
2. Click the plus (+) sign next to **Additional Installation Options** to expand the screen.



Computers > Add: Add Computers

During Agent installation, computers will be automatically added to WFBS-SVC default groups. Afterwards, you can drag and drop a computer to another group.

Note: For all installation options, this Agent is only valid for computers belonging to a single company.

Web Installation

Send the following message your clients. Either click **Copy Text** and paste it into an email, or click **Use My Default Email** to automatically insert the text into your default email application.

Click the URL to install the Trend Micro Client/Server Security Agent. The installer will guide you through the installation.

Client/Server Security Agent

Download URL:http://wfbs-svc-nabu.trendmicro.com/wfbs-svc/download/en/view/agent?type=installer&id=zajoDAkzXV3Bfx2TxP2fC2f5MJtUQd3zyWfzEq%3D%3D&lang=en

⊟ Additional Installation Options

Click the URL below to download and run the downloader which will then download the Agent Installation Package.

Download URL:http://wfbs-svc-nabu.trendmicro.com/wfbs-svc/download/en/view/agent?type=downloader&id=zajoDAkzXV3Bfx2TxP2fC2f5MJtUQd3zyWfzEq%3D%3D&lang=en

- Conventional Installation

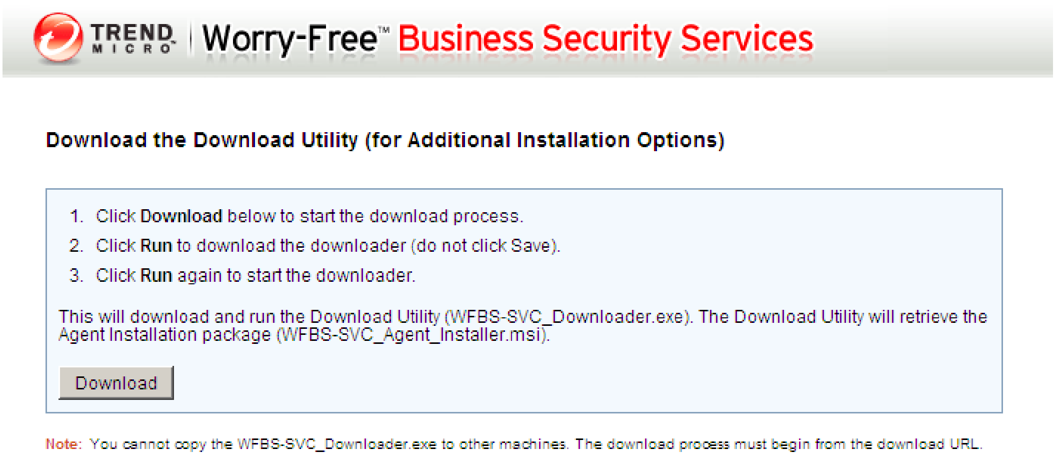
  Copy the downloaded .msi file either to each computer you wish to install the Agent on or to a shared directory on the company's local network. Double click the file to start it. The installer will guide you through the installation.

- Windows Startup Script Installation

  Get help for startup script installation

FIGURE 3-6. Download the Agent installer for conventional and scripted installation

3. When the web page opens, click **Download** to start the download process.



Download the Download Utility (for Additional Installation Options)

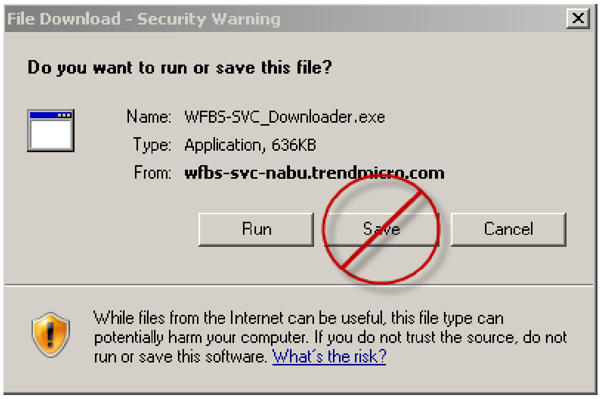
1. Click **Download** below to start the download process.
2. Click **Run** to download the downloader (do not click Save).
3. Click **Run** again to start the downloader.

This will download and run the Download Utility (WFBS-SVC_Downloader.exe). The Download Utility will retrieve the Agent Installation package (WFBS-SVC_Agent_Installer.msi).

Note: You cannot copy the WFBS-SVC_Downloader.exe to other machines. The download process must begin from the download URL.

FIGURE 3-7. Click Download to start the Agent download process

4. When the first security warning opens, click **Run**. Do not click Save. This file is only usable during this particular download process.



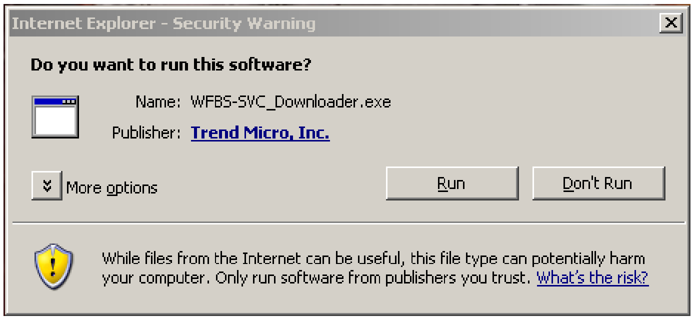
Do you want to run or save this file?

Name: WFBS-SVC_Downloader.exe
Type: Application, 636KB
From: **wfbs-svc-nabu.trendmicro.com**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

FIGURE 3-8. Click Run on the first security warning. Do not click Save.

5. When the second security warning opens, click **Run** again. This will download the Agent downloader (`WFBS-SVC_Downloader.exe`).



Do you want to run this software?

Name: WFBS-SVC_Downloader.exe
Publisher: Trend Micro, Inc.

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

FIGURE 3-9. Click Run on the second security warning

6. Once the Agent downloader has been downloaded, it will run. Click **Next** to download the Agent installer.

The `WFBS-SVC_Agent_Installer.msi` file can now be installed on each computer within the same company by:

- Copying the installer to each computer and running the file
- Running the installer from a shared directory on the company's local network
- Distributing the installer via Windows startup script

WARNING! **If you are a reseller, you must log into each company that you are administering separately to either obtain the download URL for distribution via email or to download the Agent installer for conventional or scripted installation. If you install an Agent using the wrong URL or Agent installer, the Agent will show up under the wrong customer and will have to be reinstalled using the correct installer.**

To deploy the WFBS-SVC Agent with the deployment script:

1. Download the Agent installer from **Computers > Add > Add Computers > Additional Installation Options**.
2. Place the Agent installer (`WFBS-SVC_Agent_Installer.msi)` into a folder (for example `D:\share`) on one of your servers (for example `MYFILESERVER`).
3. Share the folder (`D:\share`) using permissions so that everyone can access this folder and the WFBS-SVC Agent installer.
4. Download the example deployment script from **Administration > Tools**.
5. Open the example script (WFBS-SVC Example Deployment Script.vbs) with an editor. Modify the first line

   ```
   pathOfWFBSHInstaller="msiexec /qn /i WFBS-SVC_Agent_Installer.msi"
   ```

   to the path of your environment, for example

   ```
   pathOfWFBSHInstaller="msiexec /qn /i 
   \\MYFILESERVER\share\WFBS-SVC_Agent_Installer.msi"
   ```

6. Set the computer startup script to the path where you put the script, for example `\\MYFILESERVER\share\WFBS-SVC Example Deployment Script.vbs` (The user logon script is not used because the user may not have the necessary permission to install software).

To learn more about how to set up a windows startup script in windows domain controller, reference the following two links:

http://support.microsoft.com/kb/198642

http://technet.microsoft.com/en-us/magazine/dd630947.aspx

Verifying Agent Installation

After completing the Agent installation, verify that the Client/Server Security Agent is properly installed.

To verify the installation:

- Look for the Trend Micro Client/Server Security Agent program shortcuts on the Windows **Start** menu of the client running the Agent.
- Check if Trend Micro Client/Server Security Agent is in the **Add/Remove Programs** list of the client's Control Panel.

Testing the Client Installation with the EICAR Test Script

The European Institute for Computer Antivirus Research (EICAR) has developed a test virus you can use to test your installation and configuration. This file is an inert text file whose binary pattern is included in the virus pattern file from most antivirus vendors. It is not a virus and does not contain any program code.

Obtaining the EICAR Test File:

You can download the EICAR test virus from the following URL:

http://www.eicar.org/anti_virus_test_file.htm

Alternatively, you can create your own EICAR test virus by typing the following into a text file, and then naming the file eicar.com:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Flush the cache in the cache server and local browser before testing.

Removing Agents

There are two ways to remove Agents:

- Running the Agent uninstallation program
- Using the Web console

Removing the Agent Using the Agent Uninstallation Program

You can remove the Client/Server Security Agent with the uninstallation program.

To run the Agent uninstallation program:

1. On the Windows **Start** menu, click **Settings > Control Panel > Add or Remove Programs** (or **Programs and Features** on Windows Vista).
2. Select **Trend Micro Client/Server Security Agent** and click **Change/Remove**. The **Security Agent Uninstallation** screen appears and prompts for the uninstall password, if configured.
3. Click **OK**.

Removing the Agent Using the Web Console

You can also remotely remove Client/Server Security Agent using the Web console.

To remotely remove an Agent using the Web console:

1. Log on to the Web console.
2. Click the **Computers** tab.
3. On the Network tree, first select the group. Then, on the right pane, select the client from which you want to remove the Agent. Click **Remove**. The **Remove Computer** screen appears.
4. Click **OK**.

To verify that the Agent has been removed, refresh the **Computers** screen. The client should no longer appear on the network tree.

Chapter 4

Migrating and Upgrading

This chapter provides information to understand upgrading the Agent or migrating from other antivirus applications.

The topics discussed in this chapter include:

- *Migrating from Other Antivirus Applications* starting on page 4-2
- *Upgrading the Client/Server Security Agent* starting on page 4-5

Migrating from Other Antivirus Applications

WFBS-SVC supports migration from other antivirus applications. WFBS-SVC can automatically migrate the client software.

Migrating from Trend Micro Anti-Spyware

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

- 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. See *Table 4-1* for a comparison of the Client/Server Security Agent and TMASY anti-spyware settings.

TABLE 4-1. 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

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.

See *Table 4-2* for a list of client applications that WFBS-SVC can automatically remove.

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

TABLE 4-2. Removable Antivirus Applications

ALWIL Avast 4.6 NT	Armour Virus Control 5.8
avast! Antivirus 4.7	CA eTrust 7.1, 7.1.0194
CA eTrust InoculateIT 6.0, 7.0	CA eTrust ITM Agent 8.0, 8.1.637, 8.1.655
CA eTrustITM Server 8.0, 8.1.655	CA InocuLAN 5
CA InocuLAN NT 4.53	CA InoculateIT Clients for Windows 6.0
CA iTechnology iGateway 4.0, 4.2.0.1, 4.2.0.2	Cheyenne AntiVirus 9x, NT
Command AntiVirus for Windows 2000/XP	Command AV 4.64 9x
Command AV Enterprise 4.8, 4.9, 4.91.0, 4.93.8	Command AV Standalone 4.8, 4.9, 4.91.0, 4.93.8
Dr. Solomon 4.0.3, 4.0.3 NT, 7.77,7.95 NT	ePOAgent1000, 2000, 3000
eSafe Desktop v3	F-Prot for Windows
F-Secure 4.04, 4.08, 4.3, 5.3, 5.4x, 5.5x	F-Secure Anti-Virus 2008
F-Secure Anti-Virus for Windows Workstations 8.00, 9.00	F-Secure BackWeb
F-Secure Client Security 7.10 - E-mail Scanning	F-Secure Client Security 7.10 - Internet Shield
F-Secure Client Security 7.10 - System Control	F-Secure Client Security 7.10 - Web Traffic Scanning
F-Secure Client Security 7.10, 8.02, 9.00	F-Secure E-mail Scanning
F-Secure Internet Security 2005, 2008	F-Secure Internet Shield
F-Secure Management Agent	F-Secure Web Traffic Scan
Grisoft AVG 6.0, 7.0	Hauri VMS 2.0
Kaspersky Anti-Virus 6.0	Kaspersky Anti-Virus for Windows Workstation 5.0, 6.0
Kaspersky Anti-Virus Personal 4.0	Kaspersky Anti-Virus Workstation 3.5.5.4
Kaspersky Internet Security 7.0	LANDesk VirusProtect5.0
McAfee Anti-Spyware Enterprise 8.0	McAfee Desktop Firewall 8.0
McAfee Internet Security 6.0	Mcafee Managed VirusScan
McAfee NetShield 4.5, NT 4.03a	McAfee Security Center, 7
McAfee SecurityCenter	McAfee SpamKiller
McAfee Total Protection 3.0.0.539, 5.0	McAfee VirusScan 4.5, 4.51, 6.01, 95(1), 95(2)
McAfee VirusScan ASaP	McAfee VirusScan Enterprise 7, 7.1, 8.0, 8.5, 8.7.0.570

TABLE 4-2. Removable Antivirus Applications (Continued)

McAfee VirusScan NT	McAfee VirusScan Professional 9.0
McAfee VirusScan TC	McAfee VirusScan(MSPlus98)
McAfee WebScanX v3.1.6	Microsoft Forefront Client Security Antimalware Service 1.0.1703.0, 1.5.1941.9
Microsoft Forefront Client Security State Assessment Service 1.0.1703.0	NOD32 AV
Norman Virus Control	Norman Virus Control 5.90 Corporate
Norman Virus Control 5.90 Single User	Norton AntiVirus 2000 9x, NT, 2001 9x, 2001 NT, 2002 NT, 2003, 2003 cht, 2003 Professional, 2004, 2004 Pro, 2005, 2.0 NT, 5.0 9x, 5.0 NT, 5.31 9x, 5.31 NT, 5.32 9x, 5.32 NT, 6.524, 7.0 9x, 7.0 NT, 7.5 9x, 7.5 NT, 8.0 9x, 8.0 NT, 8.1 9x, 8.1 NT, 8.1 server
Norton AntiVirus CE 6.524, 7.0 9x, 7.0 NT, 7.5 9x, 7.5 NT, 8.0 9x, 8.0 NT, 8.1 server	Norton Internet Security 2004, 2004 JP, 2005
Panda Administrator 2006	Panda AdminSecure Reports Component
Panda Antivirus 6.0, Local Networks, Windows NT WS	Panda Cloud Office Protection 5.04.50
Panda Communication Agent 3.0 NT	Panda CVPSecure
Panda Endpoint Agent 5.02.00.0004	Panda FileSecure, Workstation
Panda Platinum 7.0	Panda Platinum Internet Security 2004/2005
Panda Titanium Antivirus 2004, 2006, 2007	Panda V10 stand alone
PER Antivirus	ServerProtect for Windows NT
Softed ViGUARD 2004 for Windows NT	Sophos Anti-Virus 9x, NT, NT 5.0, NT 7.0
Sophos AutoUpdate 1.4.0, 2.0.2	Sophos Remote Management System
Sophos Remote Update NT	Spybot Search & Destroy 1.3/1.4
Symantec AMS Server	Symantec AntiVirus 9.0.0.338, 9.0.210, 9.0.310, 9.0.410, 9.0.5.1000, 10.0.1.1000.1, 10.0.2000.2, 10.0.359.0 x64, 10.1.394.0, 10.1.394.0 DE, 10.1.4000.4, 10.1.5.5000, 10.1.5000.5 x64, 10.1.6.6000 x32, 10.1.6000.6 x64, 10.1.7000.7 x32, 10.1.7000.7 x64, 10.2.0.276, 10.2.0.298 x64, 11.0.714.839 Public Beta,
Symantec AntiVirus CE 10.0 NT	Symantec Client Firewall 2004 9x, 2004 NT
Symantec Client Security 10.1.394.0, 10.1.4000.4, 10.1.6000.6, 11.0.780.1109, 2.0.5.1000, 3.0, 3.0 NT, 3.1, 9.0.0.338/2.0.3.1000	Symantec Endpoint Protection 11.0.2000.1567, 11.0.2000.1567 - 64BIT, 11.0.2010.25, 11.0.3001.2224, 11.0.3001.2224 x64, 11.0.4000.2295, 11.0.4000.2295 x64, 11.0.780.1109, 11.0.780.1109 x64,
Symantec Packager	Symantec Quarantine Console 3.5.0

TABLE 4-2. Removable Antivirus Applications (Continued)

Symantec Quarantine Server 3.5.0	Tegam ViGUARD 9.25e for Windows NT
The Hacker Anti-Virus 5.5	Trend Micro Anti-Spyware Client for SMB 3.0, 3.2
Trend Micro Client/Server Messaging (CSM) 3.6	Trend Micro HouseCall Pro
Trend Micro HouseClean	Trend Micro Internet Security, 2008, 2009, 2009 Pro, 2009 x64, x64, 2010, 2010 Pro
Trend Micro Office Scan 7.0, 8.0, 10.0	Trend Micro PC-cillin 6, 95 1.0, 95 1.0 Lite, 97 2.0, 97 3.0, 98, 98 Plus (Win95), 98 Plus (WinNT), NT, NT 6, 2000 7.61(WinNT), 2000(Win9x), 2000(WinNT), 2002, 2003, 2004 (AV), 2004 (TIS), 2005, 2006, 2007
Trend Micro Titanium 1.0	Trend Micro Worry-Free Business Security 5.0, 5.1, 6.0
V3Pro 98, 98 Deluxe, 2000 Deluxe	ViRobot 2k Professional
ViRobot Desktop 5.5	ViRobot Expert 4.0
ViRobot ISMS client 3.5	VirusBuster 95 1.0, NT, 97, 97 Lite, 98, 98 for NT, 2000, 2000 for NT ver.1.00, 2000 for NT ver.1.20, 2001, Lite 1.0, Lite 2.0

Upgrading the Client/Server Security Agent

You can upgrade to a full version of the Agent from a previous version or from a trial version.

Preventing Upgrade for Selected Clients

Upgrading a large number of clients simultaneously can significantly increase network traffic. WFBS-SVC provides an option to prevent selected groups 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-SVC Web console, select **Computers >** {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

Web Console

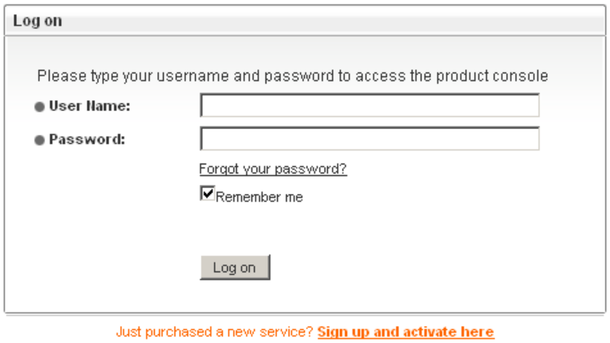
This chapter tells you how to get WFBS-SVC up and running.

The topics discussed in this chapter include:

- *Accessing the Web Console* on page 5-2
- *Live Status* on page 5-3
- *Viewing Computers and Groups* on page 5-5

Accessing the Web Console

You access the WFBS-SVC Web console using a Web browser and the provided URL.



Log on

Please type your username and password to access the product console

● User Name:

● Password:

Forgot your password?

☑ Remember me

Log on

Just purchased a new service? Sign up and activate here

FIGURE 5-1. Logon screen of WFBS-SVC

Type your user name and password in the text boxes, and then click **Log on**. The browser displays the **Live Status** screen of the Web console.

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.
Network Tree	On the **Computers** screen, the Network Tree shows desktop and server groups and allows for configuration of groups.
Security Settings toolbar	On the **Computes** screen, you can see a toolbar containing a number of icons. When you click a client or group on the Network Tree and click an icon on the toolbar, the WFBS-SVC Server performs the associated task.

Web Console Icons

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

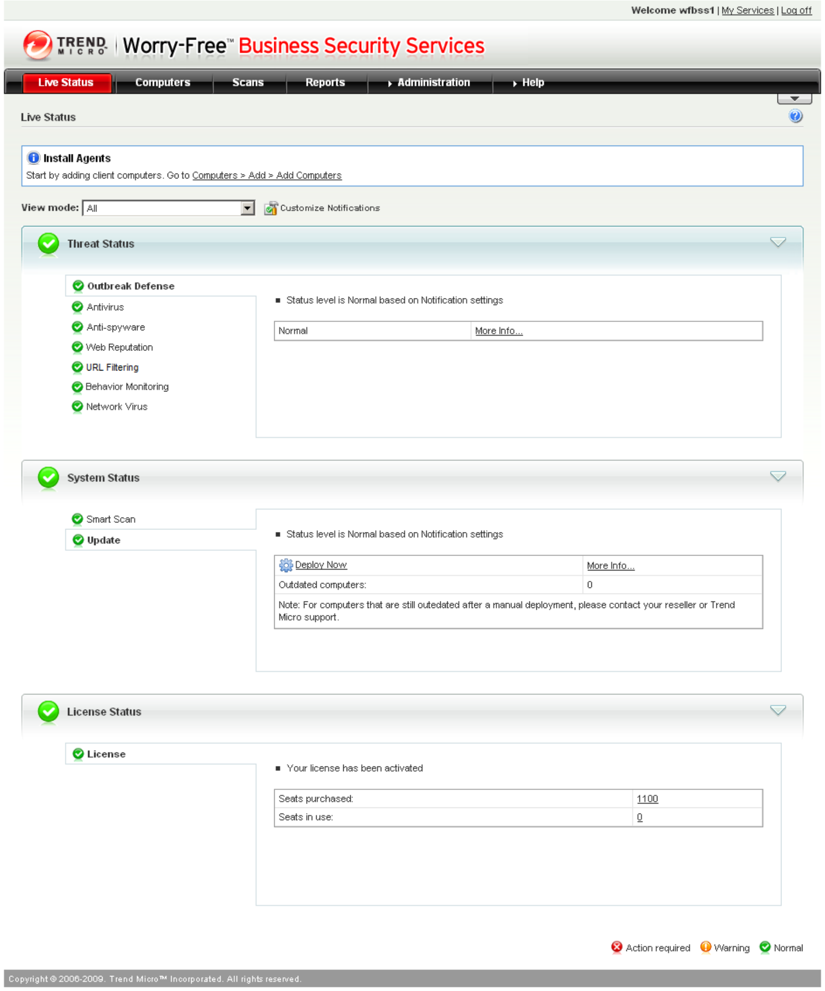
TABLE 5-2. Web Console Icons

ICON	DESCRIPTION
?	**Help** icon. Opens the online help.
✓/−	**Enable/Disable** icon. Click to enable or disable certain settings.
ℹ	**Information** icon. Displays information pertaining to a specific item.

Live Status

Use the Live Status screen to get an overall view of the threat security of your network.

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 your browser's **Refresh** button.


Welcome wfbss1 | My Services | Log off
TREND MICRO
Worry-Free™ Business Security Services
Live Status
Computers
Scans
Reports
Administration
Help

Live Status

Install Agents
Start by adding client computers. Go to Computers > Add > Add Computers

View mode: All

Customize Notifications

Threat Status

- **Outbreak Defense**
- Antivirus
- Anti-spyware
- Web Reputation
- URL Filtering
- Behavior Monitoring
- Network Virus

■ Status level is Normal based on Notification settings

Normal	More Info...

System Status

- Smart Scan
- **Update**

■ Status level is Normal based on Notification settings

Deploy Now	More Info...
Outdated computers:	0
Note: For computers that are still outedated after a manual deployment, please contact your reseller or Trend Micro support.	

License Status

- **License**

■ Your license has been activated

Seats purchased:	1100
Seats in use:	0

Action required Warning Normal

Copyright © 2006-2009. Trend Micro™ Incorporated. All rights reserved.

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.

TABLE 5-3. Live Status Icons (Continued)

ICON	DESCRIPTION
⚠	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 WFBS-SVC Server based on data collected from clients.

Status Section

The following three sections of the Live Status page are the central indicators of Trend Micro™ Worry-Free™ Business Security Services:

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:
  - **Action Unsuccessful:** 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 Scan Disabled:** Real-time scanning is disabled on Client/Server Security Agents. Click **Enable Now** to start Real-time scanning again.
- **Anti-spyware:** The Anti-spyware section displays the latest spyware scan results and spyware log entries. The number column of the Anti-Spyware table displays the results of the latest spyware scan.
  - **Spyware/Grayware Incidents:** To find more information about specific clients, click the number link in the Anti-Spyware table. From there, you can find information about the specific spyware threats that are affecting your clients.
  - Incidents Requiring Computer Restart: Click to see which computers cannot be fully cleaned until they have been restarted.
- **URL Filtering:** Restricted Web sites as determined by the Administrator. Starting from the 300th incident, the status icon changes to display a warning.
- **Web Reputation:** potentially dangerous Web sites as determined by Trend Micro. Starting from the 200th incident, the status icon changes to display a warning.
- **Behavior Monitoring:** violations of the behavior monitoring policies.
- **Network Virus:** network virus detections determined by the firewall settings.
- **Outbreak Defense:** a possible virus outbreak on your network. See *Outbreak Defense Strategy* on page 9-2 for more information.

System Status

View information regarding the updated components on computers where Agents are installed.

- **Update:** the status of Agent component updates.

Tip: You can customize the parameters that trigger the Web console to display a Warning or Action Required icon from either clicking the **Customize notifications** link at the top of the **Live Status** page or going to **Administration > Notifications**.

- **Smart Scan:** Clients that cannot connect to the Scan Server. This may indicate a network problem.
- **Component Status:** Displays updateable components and their versions.

License Status

View information regarding license status.

- **License:** information about the status of your product licenses: the number of seats purchased and the seats in use.

Viewing Computers and Groups

The **Computers** tab allows you to manage the computers on which you installed Agents. Computers are arranged by groups for administration purposes. When you select a group from the Network Tree, a table is displayed to the right listing all the computer that belong to that group. When you click the **Configure** menu item (after a group is selected from the tree), the configuration area is displayed for that group.

The Computers screen is divided into four main sections:

- Network Tree
- Group Information Table
- Menu Bar
- Configuration Area (after clicking **Configure**)

Menu Bar

Some of the following menu items will be greyed out depending on whether a group has been highlighted or not:

- **Configure:** The Configure tool is only available when one of the groups on the Network Tree is selected. The Configure tool allows you to configure settings for all Agents within that group. All computers in a group share the same configuration. You can configure the following: Scan Mode, Antivirus/Anti-spyware, Firewall, Web Reputation, Behavior Monitoring, TrendSecure Toolbars, Mail Scan and Client Privileges.
- **Add:** The Add tool allows you to add computers to specific groups by deploying Client/Server Security Agents to computers you specify.
  - **Add Group:** Add Group allows you to add new desktop or server groups.
  - **Add Computer:** Add Computers allows you to add a new computer to a group.
- **Remove:** Remove will remove the Agent from the computers that you specify.

- Others
  - **Replicate Settings:** The Replicate Settings tool is only available when one of the items on the network tree is selected and there is at least one other item of the same type in the network tree.
  - **Scan Now:** Scans all computers in a group.
  - **Stop Scan:** Stops a scan in progress.
  - **Update Now:** Updates all components
  - **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.
- **Customize Columns:** Allows you to choose only columns you want to see.

Other commands:

- **Right Click:** right clicking on a group brings up a context-sensitive menu
- **Move:** Computers may be moved from one group to another simply by dragging.

Chapter 6

Managing Groups

This chapter explains the concept and usage of groups in WFBS-SVC.

The topics discussed in this chapter include:

Overview of Groups

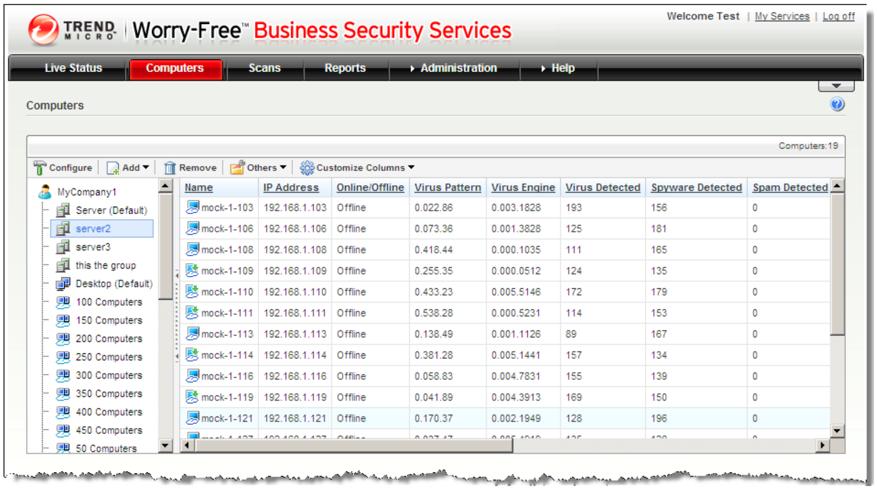
In WFBS-SVC, groups are a collection of computers and servers that share the same configuration and run the same tasks. By grouping clients, simultaneously configure, and manage, multiple Agents.

For ease of management, group clients based on the departments to which they belong or the functions they perform. Also, group clients that are at a greater risk of infection to apply a more secure configuration to all of them in just one setting.

Viewing Clients in a Group

Navigation Path: Computers > {group}

From the **Customers** tab, you can manage all clients on which you installed Client/Server Security Agents and customize security settings for Agents.



Name	IP Address	Online/Offline	Virus Pattern	Virus Engine	Virus Detected	Spyware Detected	Spam Detected
mock-1-103	192.168.1.103	Offline	0.022.86	0.003.1828	193	156	0
mock-1-106	192.168.1.106	Offline	0.073.36	0.001.3828	125	181	0
mock-1-108	192.168.1.108	Offline	0.418.44	0.000.1035	111	165	0
mock-1-109	192.168.1.109	Offline	0.255.35	0.000.0512	124	135	0
mock-1-110	192.168.1.110	Offline	0.433.23	0.005.5146	172	179	0
mock-1-111	192.168.1.111	Offline	0.538.28	0.000.5231	114	153	0
mock-1-113	192.168.1.113	Offline	0.138.49	0.001.1126	89	167	0
mock-1-114	192.168.1.114	Offline	0.381.28	0.005.1441	157	134	0
mock-1-116	192.168.1.116	Offline	0.058.83	0.004.7831	155	139	0
mock-1-119	192.168.1.119	Offline	0.041.89	0.004.3913	169	150	0
mock-1-121	192.168.1.121	Offline	0.170.37	0.002.1949	128	196	0

FIGURE 6-1. Computer tab showing clients in a group

The network tree is an expandable list of logical groups of clients. Clients are displayed according to their group on the network tree.

When you select a group from the left side and click **Configure**, the Web console displays a new configuration area.

When you select a group from the network tree on the left side, a list of the clients in the group appears to the right. Use the information on this screen to:

- Ensure your Agents are using the latest engines
- Regulate security settings depending on the number of virus and spyware incidents
- Take special action on clients with unusually high counts
- Understand overall network condition
- Verify the scan method you selected for your Agents

From here you can:

- **Configure groups:** See *Configuring Desktop and Server Groups* on page 7-2.
- **Replicate settings from one group to another:** See *Replicating Group Settings* on page 6-5.
- **Add new groups:** See *Adding Groups* on page 6-4.
- **Remove groups:** See *Removing Computers and Groups from the Web Console* on page 6-4.
- **Move Clients from one Group to another:** See *Moving Clients* on page 6-3.

Adding Clients to Groups

Worry-Free Business Security Services provides two methods to install the Client/Server Security Agent (CSA). See *Agent Installation Overview* on page 3-2

Once the Agent is installed on your client, the Agent will start to report security information to the WFBS-SVC Server.

By default, the WFBS-SVC Server refers to each client according to its computer name. You can move clients from one group to another.

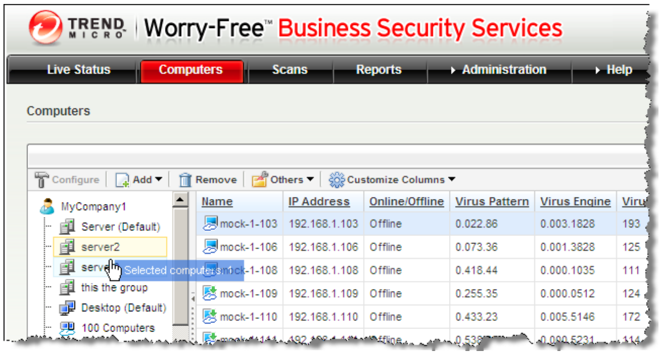
To add a Client to a Group:

1. From the **Computers** tab, click **Add > Add Computer(s)** on the toolbar.
2. Update the following as required:
    - **Method**
        - **Web Installation:** Direct download and immediate installation of the Agent See *Agent Installation - Web* on page 3-2 for more information.
        - **Additional Installation Options:** Download the Agent installer which can then be deployed via conventional installation or Windows startup script. See *Agent Installation - Additional Options* on page 3-6 for more information.
3. During Agent installation, computers will be automatically added to WFBS-SVC **Server (Default)** or **Desktop (Default)** group. You can drag and drop the computer to another group.

Moving Clients

Navigation Path: Computers > {group}

WFBS-SVC gives you the option to move clients from one Group to another.



Name	IP Address	Online/Offline	Virus Pattern	Virus Engine	Viru
mock-1-103	192.168.1.103	Offline	0.022.86	0.003.1828	193
mock-1-106	192.168.1.106	Offline	0.073.36	0.001.3828	125
ck-1-108	192.168.1.108	Offline	0.418.44	0.000.1035	111
mock-1-109	192.168.1.109	Offline	0.255.35	0.000.0512	124
mock-1-110	192.168.1.110	Offline	0.433.23	0.005.5146	172

FIGURE 6-2. Drag clients from one group to another.

To move a Client from one Group to another:

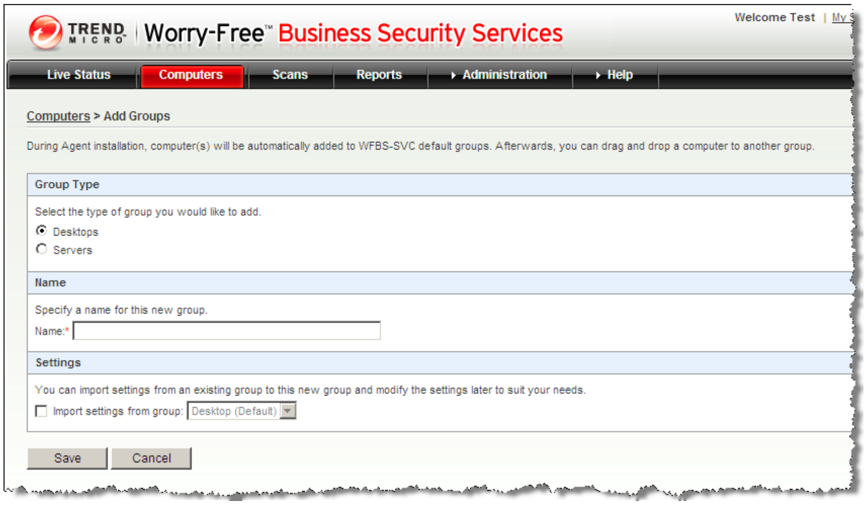
1. From the **Security Settings** screen, select the **Group**, and then select the client.
2. Drag the client into another **Group**. The client will inherit the settings of the new Group.

Adding Groups

Navigation Path: Computers > Add > Add Groups

Create groups to collectively manage multiple clients.

Note: Clients must be associated with a Group. A client cannot reside outside of a Group.



Computers > Add Groups

During Agent installation, computer(s) will be automatically added to WFBS-SVC default groups. Afterwards, you can drag and drop a computer to another group.

Group Type

Select the type of group you would like to add.

● Desktops
○ Servers

Name

Specify a name for this new group.

Name:*

Settings

You can import settings from an existing group to this new group and modify the settings later to suit your needs.

□ Import settings from group: Desktop (Default)

FIGURE 6-3. Add Group screen

To add a group:

1. From the **Add Group** screen, update the following as required:
   - **Group Type:** Select either Desktops or Servers.
   - **Group Name**
   - **Settings:** Imports security settings from an existing group.
2. Click **Save**.

Removing Computers and Groups from the Web Console

Navigation Path: Computers > {group}

You can use Remove to accomplish two goals:

- **Remove the Client icon from the Web console:** In some situations, a client might become inactive such as when the computer has been reformatted or the user disables the Client/Server Security Agent for a long time. In these situations, you might want to delete the computer icon from the Web console.
- **Uninstall the Client/Server Security Agent from a Client (and consequently remove the Client icon from the Web console):** As long as a computer or server has the Client/Server Security Agent installed, it is capable of becoming active and appearing on the Web console. To remove an inactive client for good, first uninstall the Client/Server Security Agent.

You can remove either a single computer or a group from the Web console.

WARNING! Removing the Agent from a computer may expose that computer to viruses and other malware.

To remove a Client or group:

1. Click the group or computer that you want to remove.
2. Click **Remove** from the toolbar.
3. Click **OK**.

Note: If there are still clients registered to the group, you will be unable to remove the group. Remove or uninstall the Agents before removing the group.

Removing Inactive Client/Server Security Agents

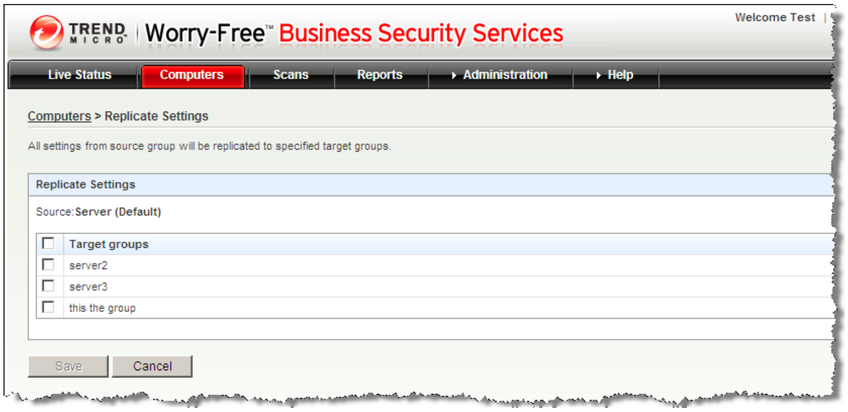
When you use the Client/Server Security Agent uninstallation program on the Client to remove the Agents from a computer, the program automatically notifies the WFBS-SVC Server. When the Server receives this notification, it removes the Client icon from the network tree to show that the Client does not exist anymore.

However, if the Client/Server Security Agent is removed using other methods, such as reformatting the computer's hard drive or deleting the Client files manually, the WFBS-SVC Server will not be aware of the removal and it will display the Client/Server Security Agent as inactive. If a user unloads or disables the Agent for an extended time, the WFBS-SVC Server also displays the Client/Server Security Agent as inactive.

Replicating Group Settings

Use Replicate Settings to copy the settings from one group on your network to another. The settings will apply to all clients that are part of the destination group.

Navigation Path: Computers > {group} > Other > Replicate Settings



Computers > Replicate Settings

All settings from source group will be replicated to specified target groups.

Replicate Settings

Source: Server (Default)

- □ Target groups
- □ server2
- □ server3
- □ this the group

FIGURE 6-4. Replicate Settings screen

To replicate settings from one group to another:

1. From the **Computers** tab, select the source Group that must replicate its settings to other Groups.
2. Click **Others > Replicate Settings**.
3. Select the target groups that will inherit settings from the source Group.
4. Click **Save**.

Chapter 7

Configuring Group Security Settings

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

The topics discussed in this chapter include:

- *Configuring Desktop and Server Groups* on page 7-2
- *Scan Methods* on page 7-2
- *Antivirus/Anti-spyware* on page 7-3
- *Firewall* on page 7-3
- *Web Reputation* on page 7-8
- *URL Filtering* on page 7-9
- *Behavior Monitoring* on page 7-10
- *TrendSecure Toolbars* on page 7-13
- *Mail Scan* on page 7-14
- *Client Privileges* on page 7-15

Configuring Desktop and Server Groups

In WFBS-SVC, 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, see *Overview of Groups* on page 6-2.

Navigation Path: Computers > {group} > Configure

The following items can be accessed by selecting a group under the network tree under the **Computers** tab and clicking **Configure**:

TABLE 7-1. Configuration Options for Desktop and Server Groups

OPTION	DESCRIPTION	DEFAULT
Scan Mode	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	Enable/Disable and configure to high, medium, or low.	Enabled, Low
URL Filtering	Enable/Disable and configure to high, medium, low, or custom.	Enabled, Low
Behavior Monitoring	Configure Behavior Monitoring options	Enabled
TrendSecure Toolbars	Enable Wi-Fi Advisor and Page Ratings	Wi-Fi Advisor: Disabled Page Ratings: Disabled
Mail Scan	Configure the scanning of POP3 email messages	Disabled
Client Privileges	Configure access to settings from the client console	N/A

Note: Other client settings, such as IM Content Filtering, apply to all clients and are accessible at **Administration > Global Settings**.

Scan Methods

Navigation Path: Computers > {Group} > Configure > Scan Method

WFBS-SVC has two methods of scanning:

- **Smart Scan:** the client uses its own scan engine, but instead of using only a local pattern file to identify threats, it primarily relies on the pattern file held on the Scan Server.
- **Conventional Scan:** the client uses its own scan engine and local pattern file to identify threats.

For more complete information, see the chapter *Scan Methods* on page 8-2

WARNING! Clients configured for Smart Scan must be online to connect with the Scan Server service. Clients configured for Smart Scan that are offline are vulnerable to threats that might already be on the computer or threats from external devices.

Antivirus/Anti-spyware

For complete Antivirus/Anti-spyware information, see the chapter *Manual Scans* on page 8-6.

Firewall

Navigation Path: Computers > {Group} > Configure > Firewall

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-SVC 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-SVC disables the Firewall on all new Groups and clients.

TABLE 7-2. Default Firewall Settings

Security Level	Description
Low	Inbound and outbound (Bi-directional) traffic allowed, only network viruses blocked.

Settings	Status
Intrusion Detection System	Disabled
Alert Message (send)	Disabled

Exception Name	Action	Direction	Protocol	Port
DNS	Allow	Bi-directional	TCP/UDP	53
NetBIOS	Allow	Bi-directional	TCP/UDP	137, 138, 139, 445
HTTPS	Allow	Bi-directional	TCP	443
HTTP	Allow	Bi-directional	TCP	80
Telnet	Allow	Bi-directional	TCP	23
SMTP	Allow	Bi-directional	TCP	25
FTP	Allow	Bi-directional	TCP	21
POP3	Allow	Bi-directional	TCP	110

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 which means that 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.

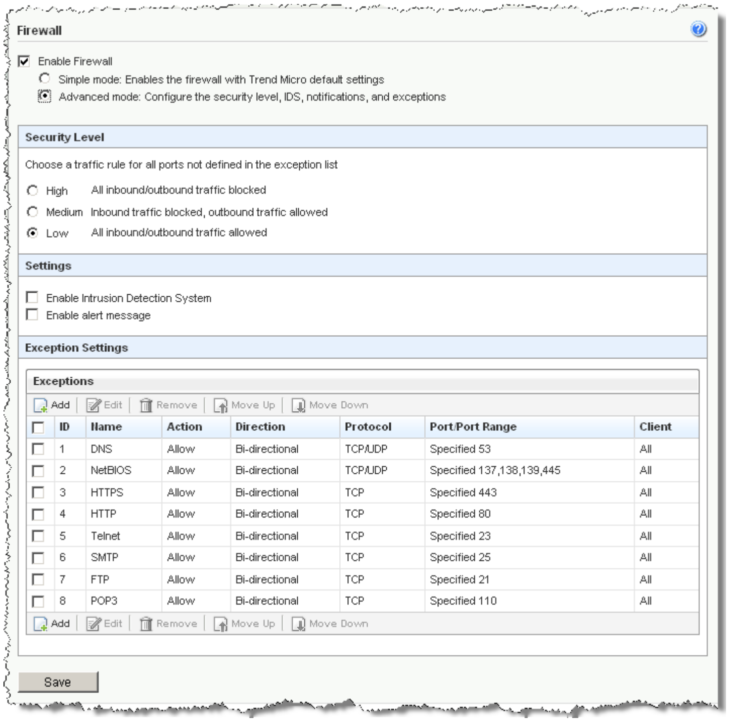
Configuring the Firewall

Navigation Path: Computers > {group} > Configure > Firewall

The Firewall was designed to protect computers from Internet threats.

Trend Micro default setting

- Firewall disabled



Firewall

☑ Enable Firewall

○ Simple mode: Enables the firewall with Trend Micro default settings

● Advanced mode: Configure the security level, IDS, notifications, and exceptions

Security Level

Choose a traffic rule for all ports not defined in the exception list

○ High All inbound/outbound traffic blocked

○ Medium Inbound traffic blocked, outbound traffic allowed

● Low All inbound/outbound traffic allowed

Settings

☐ Enable Intrusion Detection System

☐ Enable alert message

Exception Settings

Exceptions

☐	ID	Name	Action	Direction	Protocol	Port/Port Range	Client
☐	1	DNS	Allow	Bi-directional	TCP/UDP	Specified 53	All
☐	2	NetBIOS	Allow	Bi-directional	TCP/UDP	Specified 137,138,139,445	All
☐	3	HTTPS	Allow	Bi-directional	TCP	Specified 443	All
☐	4	HTTP	Allow	Bi-directional	TCP	Specified 80	All
☐	5	Telnet	Allow	Bi-directional	TCP	Specified 23	All
☐	6	SMTP	Allow	Bi-directional	TCP	Specified 25	All
☐	7	FTP	Allow	Bi-directional	TCP	Specified 21	All
☐	8	POP3	Allow	Bi-directional	TCP	Specified 110	All

FIGURE 7-1. Firewall Configuration 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. Trend Micro designed the Simple Mode to protect most small- and medium-sized businesses from Internet threats. See *Default Firewall Simple Mode Settings* on page 7-3.
     - **Advanced Mode:** Enables firewall with custom settings. Select this mode when you want to configure the settings manually. See *Advanced Firewall Options* on page 7-5 for configuration options.
2. Click **Save.** The changes take effect immediately.

Advanced Firewall Options

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

To configure advanced firewall options:

1. From the **Firewall** screen, select **Advanced Mode**.
2. Update the following options as required:
   - **Security Level:** The security level controls the traffic rules to be enforced for ports not in the exception list.
     - **High:** blocks all incoming and outgoing traffic except any traffic allowed in the exception list
     - **Medium:** blocks all incoming traffic and allows all outgoing traffic except any traffic allowed and blocked in the exception list
     - **Low:** allows all incoming and outgoing traffic except any traffic blocked in the exception list. This is the default setting for the Simple mode.
   - **Settings**
     - **Enable Intrusion Detection System:** The Intrusion Detection System identifies patterns in network packets that may indicate an attack. See *Intrusion Detection System* on page 7-7 for more information.
     - **Enable Alert Messages:** When WFBS-SVC detects a violation, the client is notified.
   - **Exceptions:** Ports in the exception list will not be blocked. See *Working with Firewall Exceptions* on page 7-5 for more information.
3. Click **Save**.

Working with Firewall Exceptions

Navigation Path: Computers > {group} > Configure > Firewall > Advanced Mode > Exception Settings

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.
   - **Port/Port Range**
     - **All ports** (default)
     - **Range**
     - **Specified ports:** Separate individual entries with commas.
   - **Machine**
     - **All IP addresses** (default)
     - **Single IP:** The IP address of a particular client.
     - **IP range**
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.
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**.

Editing Firewall Exceptions

Navigation Path: Computers > {group} > Configure > Firewall > Advanced Mode > Exception Settings {exception} > Edit

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

To edit an Exception:

1. From the Firewall Configuration screen, select the Exceptions that you want to modify.
2. Click **Edit**. The Edit Exception screen opens.
3. Change the name for the exception.

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

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.

Disabling the Firewall

Navigation Path: Computers > {group} > Configure > Firewall

To disable the Firewall:

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

Web Reputation

Navigation Path: Computers > {group} > Configure > Web Reputation

Web Reputation enhances protection against malicious Web sites. Web Reputation leverages Trend Micro's extensive Web security database to check the reputation of HTTP URLs that Clients are attempting to access or URLs embedded in email messages that are contacting Web sites.

If Web Reputation blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list. Approved URLs can only be set on a global level. For information on adding a URL to the Approved URL list, see *URL Filtering and Web Reputation* on page 11-4 for more details.

Web Reputation evaluates the potential security risk of any requested URL by querying the Trend Micro Web security database at the time of each HTTP request. Depending on the security level that has been set, it can block access to Web sites that are known or suspected to be a Web threat or unrated on the reputation database. Web Reputation provides both email notification to the administrator and online notification to the user for detections.

Reputation Score

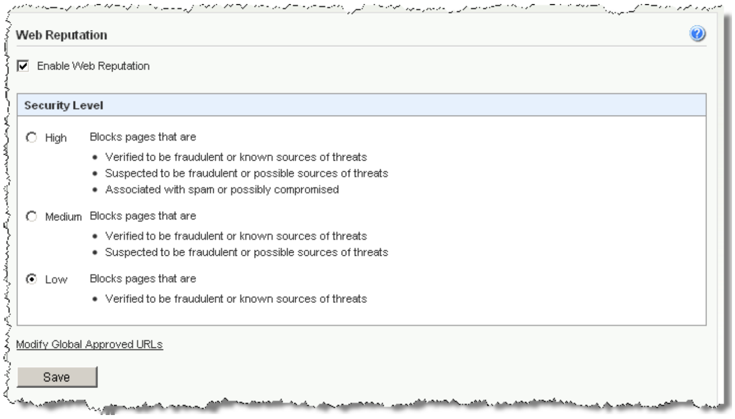
A URL's "reputation score" determines whether it is a Web threat or not. Trend Micro calculates the score using proprietary metrics.

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

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

- **High:** Blocks pages that are:
  - Verified fraud pages or threat sources
  - Suspected fraud pages or threat sources
  - Associated with spam or possibly compromised

- **Medium:** Blocks pages that are:
  - Verified fraud pages or threat sources
  - Suspected fraud pages or threat sources
- **Low (default):** Blocks pages that are verified fraud pages or threat sources



Web Reputation

☑ Enable Web Reputation

Security Level

○ High Blocks pages that are
- Verified to be fraudulent or known sources of threats
- Suspected to be fraudulent or possible sources of threats
- Associated with spam or possibly compromised

○ Medium Blocks pages that are
- Verified to be fraudulent or known sources of threats
- Suspected to be fraudulent or possible sources of threats

● Low Blocks pages that are
- Verified to be fraudulent or known sources of threats

FIGURE 7-2. Web Reputation configuration

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**.

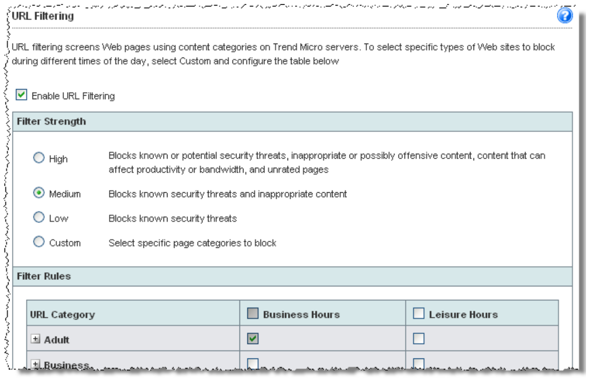
URL Filtering

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

Configuring URL Filtering

Navigation Path: Computers > {Group} > Configure > URL Filtering

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



URL Filtering

URL filtering screens Web pages using content categories on Trend Micro servers. To select specific types of Web sites to block during different times of the day, select Custom and configure the table below

☑ 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 specific page categories to block

Filter Rules

URL Category	▨ Business Hours	□ Leisure Hours
⊞ Adult	☑	□
⊞ Business	□	□

FIGURE 7-3. Security Settings > URL Filtering screen

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

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

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

4. **Business Hours**: Any days or hours that are not defined under Business Hours are considered Leisure hours.
5. Click **Save**.

Behavior Monitoring

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

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

TABLE 7-3. 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 7-3. Possible Changes Monitored

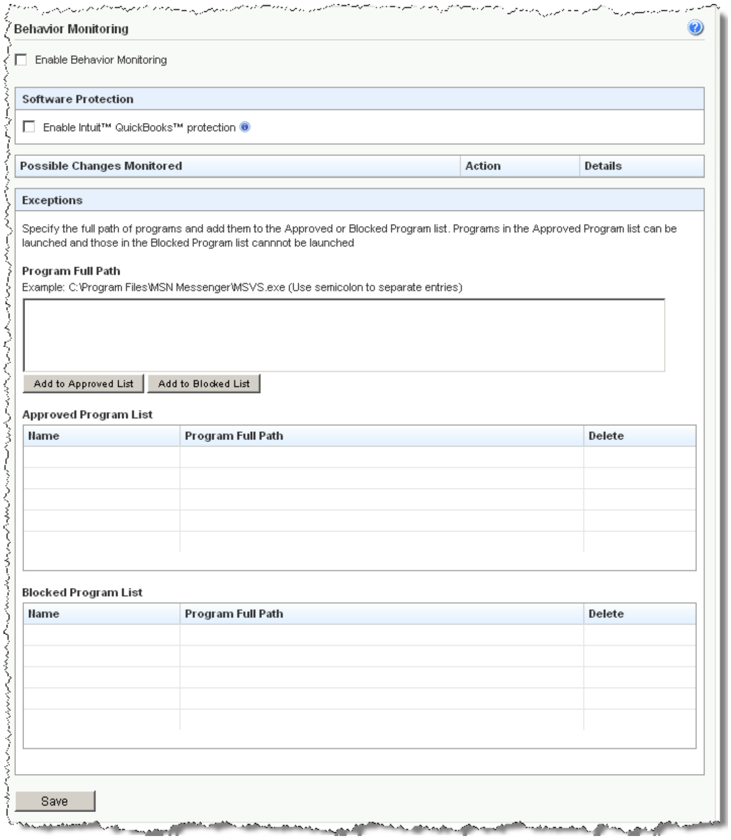
MONITORED CHANGE	DESCRIPTION	DEFAULT VALUE
Hosts File Modification	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the Web browser is redirected to infected, non-existent, or fake Web sites.	Always block
System File Modification	Certain Windows 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
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
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: Computers > {group} > Configure > Behavior Monitoring

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



Behavior Monitoring

□ Enable Behavior Monitoring

Software Protection

□ Enable Intuit™ QuickBooks™ protection

Possible Changes Monitored	Action	Details

Exceptions

Specify the full path of programs and add them to the Approved or Blocked Program list. Programs in the Approved Program list can be launched and those in the Blocked Program list cannot be launched

Program Full Path

Example: C:\Program Files\MSN Messenger\MSVS.exe (Use semicolon to separate entries)

Approved Program List

Name	Program Full Path	Delete

Blocked Program List

Name	Program Full Path	Delete

FIGURE 7-4. Behavior Monitoring screen

To edit Behavior Monitoring settings:

1. From the **Behavior Monitoring** screen, update the following as required:
   - **Enable Behavior Monitoring**
   - **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
   - **Possible Changes Monitored:** Select **Always Allow**, **Ask When Necessary**, or **Always Block** for each monitored change. See Table 7-3 on page 7-10 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 path of the program. Separate multiple entries with semicolons (;). Click **Add to Approved Programs List** or **Add to Blocked Programs List**.
  - **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**.

Viewing Computers Violating Behavior Monitoring Policies

Navigation Path: Live Status > Behavior Monitoring > {number of incidents}

The information displayed in the Policy Violations Detected screen is generated or updated whenever a computer violates a behavior monitoring policy. Click Reset to clear all previous records. The next time a URL is blocked, it will appear in this screen.

- **Computer Name:** Name of the computer attempting violating a policy. Click the name to see a list of the time of violation, the program violation the policy, the affected program, and the action taken on the violation program.
- **Number of Detections:** Number of violations.

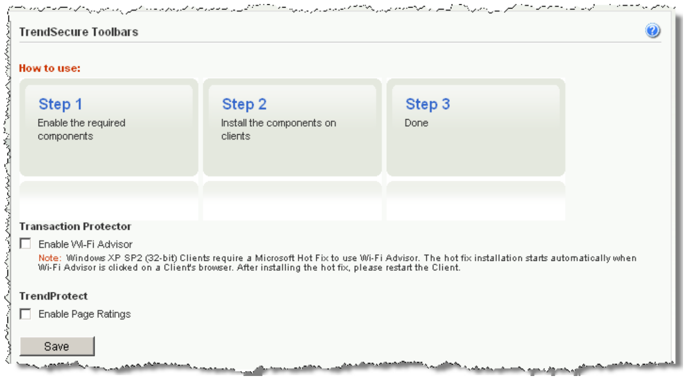
TrendSecure Toolbars

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.

Navigation Path: Computers > {group} > Configure > TrendSecure Toolbars



TrendSecure Toolbars

How to use:

Step 1
Enable the required components

Step 2
Install the components on clients

Step 3
Done

Transaction Protector

□ Enable Wi-Fi Advisor

Note: Windows XP SP2 (32-bit) Clients require a Microsoft Hot Fix to use Wi-Fi Advisor. The hot fix installation starts automatically when Wi-Fi Advisor is clicked on a Client's browser. After installing the hot fix, please restart the Client.

TrendProtect

□ Enable Page Ratings

FIGURE 7-5. TrendSecure Toolbars - In Office screen

To configure the availability of TrendSecure tools:

1. From the **TrendSecure Toolbars** 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.

Mail Scan

The POP3 Mail Scan plug-in protects clients in real-time against security risks and spam transmitted through POP3 email messages.

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 (Windows XP only)
- Windows Mail™ (Microsoft Vista only)
- Mozilla Thunderbird 1.5 and 2.0

Navigation Path: Computers > {group} > Configure > Mail Scan

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.

To edit the availability of Mail Scan:

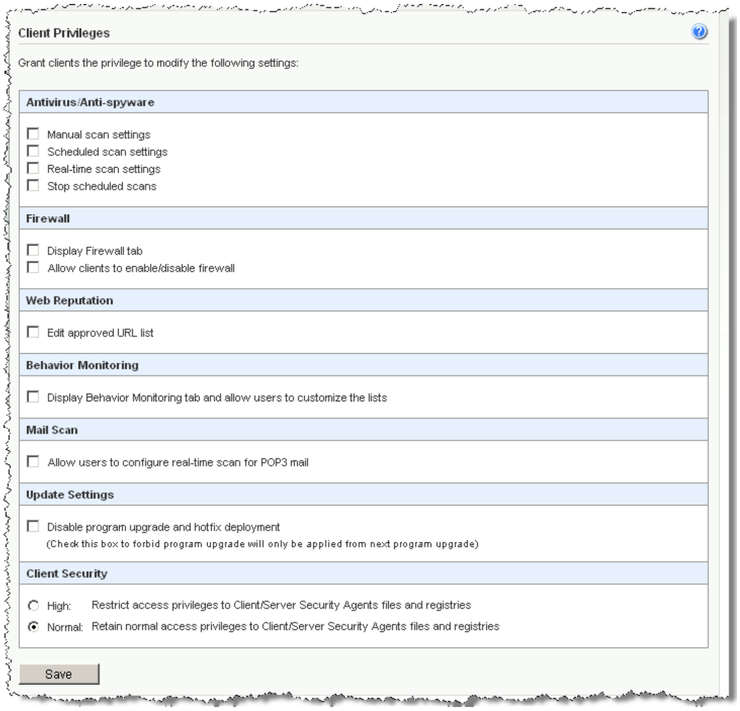
1. From the Mail Scan screen, update the following as required:
    - Enable real-time scan for POP3 mail
    - Enable Trend Micro Anti-Spam toolbar
2. Click **Save**.

Client Privileges

Navigation Path: Computers > {group} > Configure > Client Privileges

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

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



Client Privileges

Grant clients the privilege to modify the following settings:

Antivirus/Anti-spyware

- □ Manual scan settings
- □ Scheduled scan settings
- □ Real-time scan settings
- □ Stop scheduled scans

Firewall

- □ Display Firewall tab
- □ Allow clients to enable/disable firewall

Web Reputation

- □ Edit approved URL list

Behavior Monitoring

- □ Display Behavior Monitoring tab and allow users to customize the lists

Mail Scan

- □ Allow users to configure real-time scan for POP3 mail

Update Settings

- □ Disable program upgrade and hotfix deployment
  (Check this box to forbid program upgrade will only be applied from next program upgrade)

Client Security

- ○ High: Restrict access privileges to Client/Server Security Agents files and registries
- ● Normal: Retain normal access privileges to Client/Server Security Agents files and registries

FIGURE 7-6. 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**
   - **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, 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**
- **Update Settings**
  - **Disable program upgrade and hotfix deployment**
- **Client Security**
  - **High:** Prevents access to Agent folders, files, and registry entries.
  - **Normal:** Provides 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**.

Chapter 8

Managing Scans

This chapter describes how to use the various types of scans to protect your network and clients from virus/malware and other threats.

The topics discussed in this chapter include:

About Scanning

WFBS-SVC provides two scan methods and three types of scans to protect your clients from Internet threats:

- Smart Scan
- Conventional Scan
    - Manual Scan
    - Scheduled Scan
    - Real-time Scan.

Each scan has a different purpose and use, but all are configured approximately the same way.

Scan Methods

Navigation Path: Computers > {Group} > Configure > Scan Method

Scan methods consist of:

- **Smart Scan:** the client uses its own scan engine, but instead of using only a local pattern file to identify threats, it primarily relies on the pattern file held on the Scan Server.
- **Conventional Scan:** the client uses its own scan engine and local pattern file to identify threats.

WARNING! **Clients configured for Smart Scan must be online to connect with the Scan Server service. Clients configured for Smart Scan that are offline are vulnerable to threats that might already be on the computer or threats from external devices.**

If client scans are slowing down client computers, consider switching to Smart Scan. By default, Smart Scan is enabled. You can disable Smart Scan for groups of clients by going to **Computers** > {Group} **> Configure** > **Scan Method**. Click **Smart Scan** or **Conventional Scan**.

Scan Types

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-SVC 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.
- **Manual Scan:** Manual Scan is an on-demand scan. This scan also eradicates old infections that may be lying dormant in files 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.

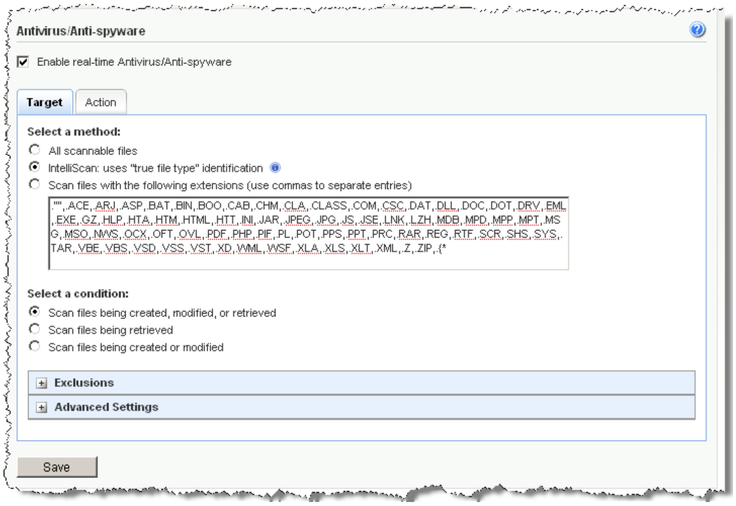
- **Scheduled Scan:** A Scheduled Scan is similar to Manual Scan but scans all files at the configured time and frequency. Use Scheduled Scans to automate routine scans on your clients and improve the efficiency of threat management.

To configure a Scheduled scan, click **Scans** > **Scheduled Scan**. See *Scheduled Scans* on page 5 for more information.

Note: Do not confuse the scan types above with Scan Mode. The Scan Mode refers to Smart Scan and Conventional Scan (*Scan Methods* on page 8-2).

Configuring Real-time Scan

Navigation Path: Computers > {group} > Configure > Antivirus/Anti-spyware



Antivirus/Anti-spyware

☑ Enable real-time Antivirus/Anti-spyware

Target | Action

Select a method:

○ All scannable files

● IntelliScan: uses "true file type" identification

○ Scan files with the following extensions (use commas to separate entries)

."",.ACE,.ARJ,.ASP,.BAT,.BIN,.BOO,.CAB,.CHM,.CLA,.CLASS,.COM,.CSC,.DAT,.DLL,.DOC,.DOT,.DRV,.EML,.EXE,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JPEG,.JPG,.JS,.JSE,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSO,.NWS,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.POT,.PPS,.PPT,.PRC,.RAR,.REG,.RTF,.SCR,.SHS,.SYS,.TAR,.VBE,.VBS,.VSD,.VSS,.VST,.XD,.WML,.WSF,.XLA,.XLS,.XLT,.XML,.Z,.ZIP,.{*

Select a condition:

● Scan files being created, modified, or retrieved

○ Scan files being retrieved

○ Scan files being created or modified

FIGURE 8-1. Computers > {group} > Configure > 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**
   - **Select a method:**
     - **All scannable files:** Only encrypted or password-protected files are excluded.
     - **IntelliScan:** Scans files based on true-file type. See *Trend Micro IntelliScan* on page B-2 for more information.
     - **Scan files with the following extensions:** WFBS-SVC will scan files with the selected extensions. Separate multiple entries with commas (,).
   - **Select a condition**:
     - **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 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 directories where Trend Micro products are installed**

  - **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 **Administration > Global Settings > General Scan Settings** and 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. See *Trend Micro IntelliTrap* on page B-3 for more information.
  - **Scan mapped drives and shared folders on the network** (for antivirus)
  - **Scan floppy drive system shutdown** (for antivirus)
  - **Scan layer(s) of 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. See *Editing the Spyware/Grayware Approved List* on page 8-9 for more information.

2. From the **Action** tab on the **Antivirus/Anti-spyware** screen, specify how WFBS-SVC should handle detected threats:
   - **For Virus Detections**
     - **ActiveAction:** Use Trend Micro preconfigured actions for threats. See *Trend Micro ActiveAction* on page B-2 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
       ```
   - **For Spyware/Grayware Detections**
     - **Clean:** When cleaning spyware/grayware, WFBS-SVC 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. See *Configuring Alert Thresholds* on page 10-3.

Enabling Real-Time Scan

By default, Real-time scanning is enabled for both antivirus and anti-spyware.

WARNING! If you disable real-time scanning, your desktops and servers become vulnerable to infected files.

To enable Real-time scanning on the Client:

1. Click **Computers >** {group} **> Configure**.
2. Click **Antivirus/Anti-spyware**.
3. Click **Enable real-time Antivirus/Anti-spyware**. The WFBS-SVC Server sends a notification to the Client/Server Security Agent to enable Real-time scanning.

Note: Real-time anti-spyware scan is dependant on real-time antivirus scan. So, you cannot enable only real-time anti-spyware scan.

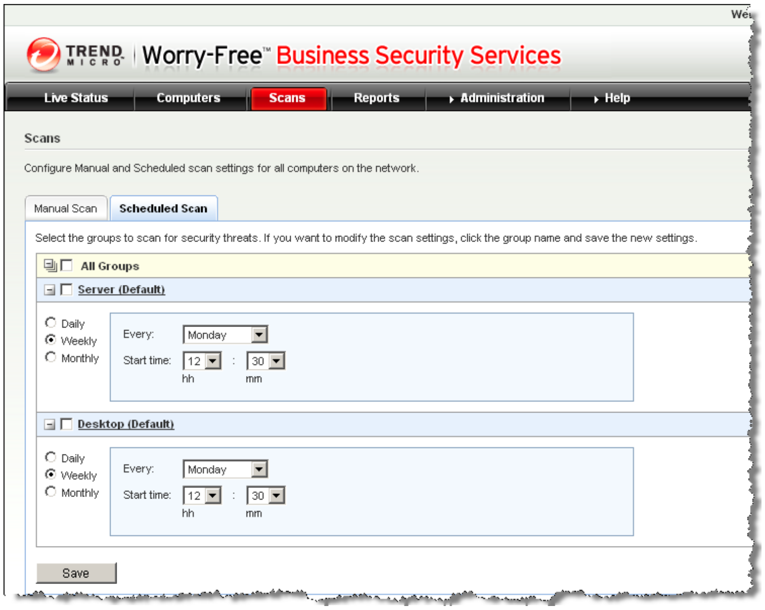
Scheduled Scans

Navigation Path: Scans > Scheduled Scan

Schedule scans to periodically scan clients for threats.

Tip: If you begin a Manual Scan when a Scheduled Scan is running, the Scheduled Scan will abort, but runs again according to its schedule.

Note: To disable Scheduled Scan, clear the checkbox next to the name of the group and click **Save**.



Scans

Configure Manual and Scheduled scan settings for all computers on the network.

Select the groups to scan for security threats. If you want to modify the scan settings, click the group name and save the new settings.

□ All Groups

□ Server (Default)

○ Daily
● Weekly
○ Monthly

Every: Monday

Start time: 12 hh : 30 mm

□ Desktop (Default)

○ Daily
● Weekly
○ Monthly

Every: Monday

Start time: 12 hh : 30 mm

FIGURE 8-2. Scheduled Scan screen

All groups from the network tree under the **Computers** tab are listed on this page.

To schedule a scan:

1. Before scheduling a scan, configure the settings for the scan. See *Configuring Manual and Scheduled Scans* on page 8-7 for more information.
2. From the **Scheduled Scan** tab, update the following options for each group as required:
   - **Daily:** The Scheduled Scan runs every day at the **Start time**.
   - **Weekly, every:** The Scheduled Scan runs once a week on the specified day at the **Start time**.
   - **Monthly, on day:** The Scheduled Scan runs once a month on the specified day at the **Start time**.

   WARNING! **If you select day 31 and the month has only 30 days, WFBS-SVC will not perform the scan that month.**

   - **Start time:** The time the Scheduled Scan should start.
3. Click **Save**.

   Additionally, configure who receives notifications when an event occurs. See *Configuring Alert Thresholds* on page 10-3.

Tip: Trend Micro recommends scheduling scans at regular intervals for optimal protection.

Manual Scans

Navigation Path: Scans > Manual Scan

The **Manual Scan** screen lists all your computer groups. Clicking a group name takes you to a new screen that allows you to configure the scan.

Manual Scan scans all specified groups. To perform a manual scan, select the groups to scan and the items to scan for. Click **Scan Now** to start a scan and **Stop Scanning** to end a manual scan.

The Client/Server Security Agent uses Trend Micro recommended settings when scanning for viruses and other malware. When it detects a security threat, it automatically takes action against those threats according to these settings and logs the actions.

You can view the results in the **Live Status** screen or by generating reports or log queries.

To run a manual scan:

1. Click **Scans > Manual Scan**.
2. Configure settings as desired by clicking on the group name (see *Configuring Manual and Scheduled Scans* on page 8-7)
3. Select a group or groups to scan.
4. Click **Scan Now**. The Scan Notifying Progress screen appears. When the scan is complete, the Scan Notifying Results screen appears.

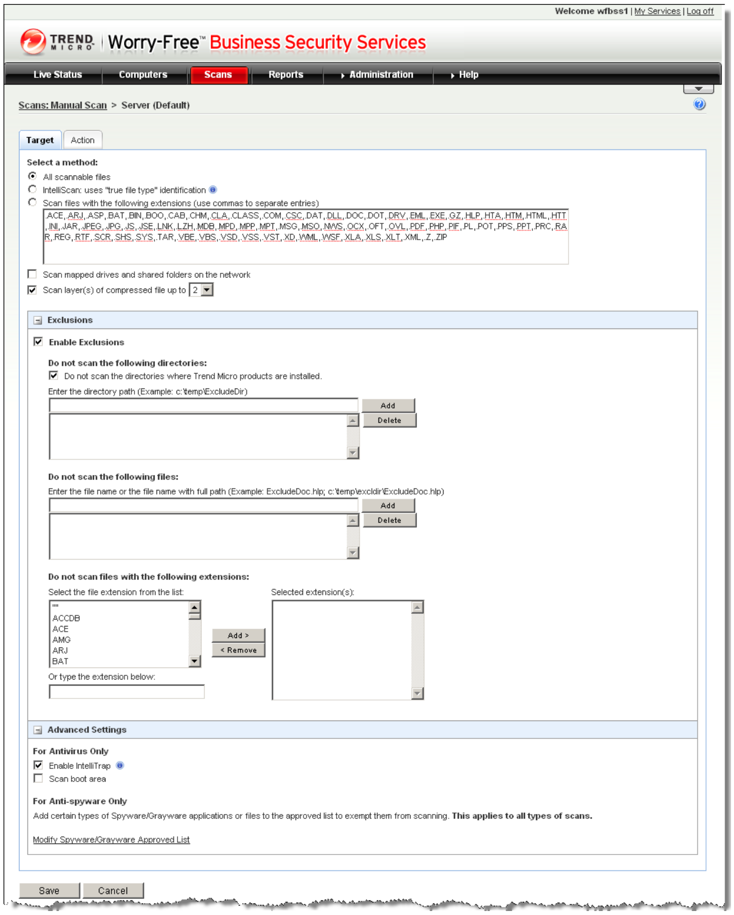
Configuring Manual and Scheduled Scans

Configuring Scan Options involves setting the Target (files to scan) and the Action (action for detected threats).

Navigation Path: Scans > Manual Scan OR Scheduled Scan > {group}

Scheduled scans for Client/Server Security Agents are disabled by default. If you enable Scheduled scans, Trend Micro recommends that you schedule scans to run during an off-peak time for your Clients.

First set the target (**Target** tab) files to scan, including optional settings, and then set the actions (**Action** tab) for the Client/Server Security Agent (CSA) to take against detected threats.



Scans: Manual Scan > Server (Default)

Select a method:

● All scannable files

○ IntelliScan: uses "true file type" identification

○ Scan files with the following extensions (use commas to separate entries)

.ACE,.ARJ,.ASP,.BAT,.BIN,.BOO,.CAB,.CHM,.CLA,.CLASS,.COM,.CSC,.DAT,.DLL,.DOC,.DOT,.DRV,.EML,.EXE,.GZ,.HLP,.HTA,.HTM,.HTML,.HTT,.INI,.JAR,.JPEG,.JPG,.JS,.JSE,.LNK,.LZH,.MDB,.MPD,.MPP,.MPT,.MSG,.MSO,.NWS,.OCX,.OFT,.OVL,.PDF,.PHP,.PIF,.PL,.POT,.PPS,.PPT,.PRC,.RAR,.REG,.RTF,.SCR,.SHS,.SYS,.TAR,.VBE,.VBS,.VSD,.VSS,.VST,.XD,.WML,.WSF,.XLA,.XLS,.XLT,.XML,.Z,.ZIP

□ Scan mapped drives and shared folders on the network

☑ Scan layer(s) of compressed file up to 2

Exclusions

☑ **Enable Exclusions**

Do not scan the following directories:

☑ Do not scan the directories where Trend Micro products are installed.

Enter the directory path (Example: c:\temp\ExcludeDir)

Do not scan the following files:

Enter the file name or the file name with full path (Example: ExcludeDoc.hlp; c:\temp\excldir\ExcludeDoc.hlp)

Do not scan files with the following extensions:

Select the file extension from the list:

""
ACCDB
ACE
AMG
ARJ
BAT

Selected extension(s):

Or type the extension below:

Advanced Settings

For Antivirus Only

☑ Enable IntelliTrap

□ Scan boot area

For Anti-spyware Only

Add certain types of Spyware/Grayware applications or files to the approved list to exempt them from scanning. **This applies to all types of scans.**

Modify Spyware/Grayware Approved List

FIGURE 8-3. Scan Options

To configure the scan options:

1. On the **Target** tab, update the following as required:
   - Files to scan
     - **All scannable files:** Only encrypted or password-protected files are excluded.
     - **IntelliScan:** Scans files based on true-file type. See *Trend Micro IntelliScan* on page B-2 for more information.
     - **Scan files with the following extensions:** WFBS-SVC will scan files with the selected extensions. Separate multiple entries with commas (,).

  - **Scan mapped drives and shared folders on the network**
  - **Scan layer(s) of compressed file up to __:** Deeper than the indicated number, the file will not be scanned.
- **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**
    - **Folder exclusions:** Type the name of the folder to exclude from the scan. Click **Add.** To remove a folder, select the folder and click **Delete**.
    - **File exclusions:** Type the name of the file to exclude from the scan. Click **Add.** To remove a file, select the file and click **Remove**.
    - **Extension exclusions:** Type the name of the extension to exclude from the scan. Click **Add.** To remove an extension, select the extension and click **Remove**.
- **Advanced Settings**
  - **Enable IntelliTrap** (for antivirus)**:** IntelliTrap detects malicious code such as bots in compressed files. See *Trend Micro IntelliTrap* on page B-3 for more information.
  - **Scan boot area**
  - **Modify Spyware/Grayware Approved List** (for anti-spyware)**:** This list contains details of the approved spyware/grayware applications. Click the link to update the list. See *Editing the Spyware/Grayware Approved List* on page 8-9 for more information.

2. On the **Action** tab, specify how WFBS-SVC should handle CPU usage and detected threats:

- **CPU usage:** Set to High, Medium, or Low. The default setting is High for the shortest scanning time.
- **For Virus Detections**
  - **ActiveAction:** Use Trend Micro preconfigured actions for threats. See *Trend Micro ActiveAction* on page B-2 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.

    - *Quarantine* is the default action for **Joke**, **Worms/Trojans**, and **Packer**
    - *Clean* is the default action for **Viruses and Other Threats**
    - *Pass* is the default action for **Test Viruses**
  - **Backup detected file before cleaning:** WFBS-SVC makes a backup of the threat before cleaning. The backed-up file is encrypted and stored in the following directory on the client:

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

    To decrypt the file, see *Restore Encrypted Virus* on page 14-2
- **For Spyware/Grayware Detections**
  - **Clean:** When cleaning spyware/grayware, WFBS-SVC could delete related registry entries, files, cookies, and shortcuts. Processes related to the spyware/grayware could also be terminated.
  - **Pass:** Perform no action other than recording the detected spyware in the log files for assessment

3. Click **Save**.

Default Manual Scan settings recommended by Trend Micro

- Files to scan
  - **All scannable:** Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.
  - **Scan boot area:** Scans the boot sector of the hard disk on the Client.
  - **Scan compressed files up to 2 compression layers:** Scans compressed files that are 1 or 2 compression layers deep.
  - **Do not scan the directories where Trend Micro products are installed:** Will not scan folders containing Trend Micro products.
- Actions on detected threats
  - **CPU usage:** The default setting is High for the shortest scanning time.
  - **Perform the same action for all detected Internet threats:** Cleans all threats or deletes the threat if it is uncleanable.
  - **Backup detected file before cleaning:** Saves a copy of the detected file to the backup directory on the Client before performing action.

Editing the Spyware/Grayware Approved List

Certain applications are classified by Trend Micro as spyware/grayware not because they can cause harm to the system on which they are installed, but because they have the potential to expose the Client or the network to malware or hacker attacks. Worry-Free Business Security Services includes a list of potentially risky applications and, by default, prevents these applications from executing on Clients.

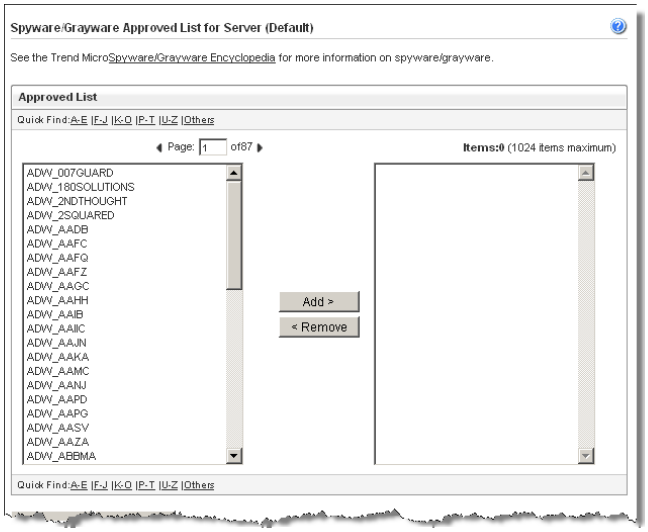
By preventing potentially risky applications from running and giving you full control over the spyware/grayware approved list, WFBS-SVC helps ensure that only the applications you approve run on Clients and servers.

If Clients need to run any application that is classified by Trend Micro as spyware/grayware, you need to add the application name to the spyware/grayware approved list.

The Spyware/Grayware Approved List determines which spyware or grayware applications users can use. See *Spyware/Grayware* on page 1-10 to learn about the different kinds of spyware.

Note: For a particular group, the same list is used for Real-Time, Scheduled, and Manual Scans.

Navigation Path: Scans > {group} > Target > Advanced Settings > Modify Spyware/Grayware Approved List



Spyware/Grayware Approved List for Server (Default)

See the Trend MicroSpyware/Grayware Encyclopedia for more information on spyware/grayware.

Approved List

Page: 1 of87

Items:0 (1024 items maximum)

ADW_007GUARD
ADW_180SOLUTIONS
ADW_2NDTHOUGHT
ADW_2SQUARED
ADW_AADB
ADW_AAFC
ADW_AAFQ
ADW_AAFZ
ADW_AAGC
ADW_AAHH
ADW_AAIB
ADW_AAIIC
ADW_AAJN
ADW_AAKA
ADW_AAMC
ADW_AANJ
ADW_AAPD
ADW_AAPG
ADW_AASV
ADW_AAZA
ADW_ABBMA

Quick Find:A-E |F-J |K-O |P-T |U-Z |Others
Add >
< Remove
Quick Find:A-E |F-J |K-O |P-T |U-Z |Others

FIGURE 8-4. Spyware/Grayware Approved List screen

To update the Spyware/Grayware Approved List:

1. From the **Spyware/Grayware Approved List** screen, update the following as required:
   - **Left pane:** Recognized spyware or grayware applications. Use **Quick Find** links to locate the spyware/grayware application that you want to allow.

   Note: Applications are sorted by type of the application and then application name (SpywareType_ApplicationName).

   - **Right pane:** Approved spyware or grayware applications.
   - **Add >:** Select the application name in the left pane and click **Add >**. To select multiple applications, press CTRL while clicking the application names.
2. Click **Save**.

Excluding Files and Folders from Scans

To increase the performance of scanning and to skip files that are causing false alarms, you can exclude certain files and folders from scanning. The files and folders you add to the exclusion list will be skipped by Manual Scan, Real-time scan, and Scheduled Scan.

Tip: The WFBS-SVC Server may detect several commonly used applications, such as Hotbar, and interpret them as threats. To prevent the Agent from detecting commonly used applications, add the application files to the Exclusion List for all types of scans.

To exclude files and folders from scans:

1. On the main menu, click **Computers >** {group} **> Configure** > **Antivirus/Anti-spyware**.
2. Click the expand button next to the **Exclusions** section of the **Antivirus/Anti-spyware page**.
3. Under **Exclusions**, make sure that the check box next to **Enable Exclusions** is selected.

4. To exclude all folders containing Trend Micro products and components, select the **Do not scan the directories where Trend Micro products are installed** check box.
5. To exclude specific directories, type the directory names under Enter the directory path (E.g. c:\temp\ExcludeDir) and click **Add**.
6. To exclude specific files by file name, type the file names, or the file name with full path under **Enter the file name or the file name with full directory path** (E.g. ExcludeDoc.hlp; c:\temp\excldir\ExcludeDoc.hlp) and click **Add**.

Note: All subdirectories in the directory path you specify will also be excluded.

7. Specify the files to exclude based on their extensions. To use specified extensions, select the extensions to protect from the Select file extension from the list, and click **Add**. To specify an extension that is not in the list, type the extension below the text box, and then click **Add**.

Note: Wildcard characters, such as "*", are not accepted for file extensions.

8. Click **Save**.

Viewing Unsuccessful Action on Desktops and Servers

Navigation Path: Live Status > Threat Status > Antivirus > Action unsuccessful

The information displayed in this section is generated or updated whenever a Real-time, Manual, or Scheduled scan occurs. Click Reset to clear all previous records. The next time a scan detects a virus or malware, it will appear in this screen.

The Viruses Detected at Desktops/Servers screen contains the following information:

- **Date/Time:** Date and time of last unsuccessful attempt to clean or remove the virus or malware.
- **Computer Name:** Name of computer infected with virus/malware.
- **Virus/Malware Name:** Click the link to be redirected to the Trend Micro virus encyclopedia for an in-depth description of the virus or malware including instructions to manually clean attacks by this particular threat.
- **File Name:** Name of file corrupted by virus/malware.
- **Path:** The location of the file.
- **Scan Type:** Type of scan used to detect the virus/malware.
- **Action Taken:** Action taken in response to detected virus/malware.

Incidents Requiring Computer Restart

Navigation Path: Live Status > Threat Status > Anti-spyware > Incidents Requiring Computer Restart

The Client/Server Security Agent detected spyware or grayware on these computers and took action to remove the spyware/grayware. In order to completely remove some spyware/grayware programs, a computer restart is required.

The following commands are available:

- **Export:** Exports the items in the table to a CSV file.
- **Reset:** Resets the Computer Restart Required for Spyware/Grayware Cleaning table. The information in the Live Status screen will also be reset.

The screen contains the following information:

- **Date/Time:** Represents the time that the Client/Server Security Agent uploaded the spyware detection information to the Security Server.
- **Computer Name:** Name of the computer that needs to be restarted.
- **Spyware/Grayware Name:** Name of the Spyware/Grayware. Clicking the spyware/grayware name will open the Trend Micro Virus and Spyware encyclopedia in a new browser window.
- **Scan Type:** Scan type that detected the spyware/grayware.

Chapter 9

Using Outbreak Defense

This chapter explains the Outbreak Defense Strategy, how to configure Outbreak Defense, and how to use it to protect networks and clients.

The topics discussed in this chapter include:

- *Outbreak Defense Strategy* on page 9-2
- *Outbreak Defense Details* on page 9-3
- *Outbreak Alert Settings* on page 9-4

Outbreak Defense Strategy

Outbreak Defense is a key component of the WFBS-SVC solution and protects your business during a worldwide threat outbreak.

The Outbreak Defense Strategy is based on the idea of an Internet-wide outbreak life cycle. The life of an outbreak is divided into three stages — **Threat Prevention**, **Threat Protection**, and **Threat Cleanup**. Trend Micro counters each stage of the cycle with a defense strategy called Outbreak Defense.

TABLE 9-1. Outbreak Defense Response to the Outbreak Life Cycle Stages.

OUTBREAK STAGE	OUTBREAK DEFENSE STAGE
In the first stage of an outbreak cycle, the experts at Trend Micro observe a threat that is actively circulating on the Internet. At this time, there is no known solution for the threat.	**Threat Prevention** Outbreak Defense prevents the threat from attacking your computers and network by taking actions according to the Outbreak Policy downloaded from Trend Micro update servers. These actions include sending alerts, blocking ports and denying access to folders and files.
In the second stage of the outbreak, computers that have been affected by the threat pass the threat along to other computers. The threat begins to rapidly spread through local networks causing business interruptions and damaging computers.	**Threat Protection** Outbreak Defense protects at-risk computers by notifying them to download the latest components and patches.
In the third and final stage of an outbreak, the threat subsides with fewer reported incidents.	**Threat Cleanup** Outbreak Defense repairs damage by running Cleanup services. Other scans provide information that Administrators can use to prepare for future threats.

Outbreak Defense Actions

The Outbreak Defense Strategy was designed to manage outbreaks at every point along the outbreak life cycle. Based on the Outbreak Prevention Policy, Automatic Threat Response typically takes pre-emptive steps such as:

- Blocking shared folders to help prevent virus/malware from infecting files in shared folders
- Blocking ports to help prevent virus/malware from using vulnerable ports to spread the infection on the network and clients

Note: Outbreak Defense never blocks the port used by the WFBS-SVC Server to communicate with clients.

- Denying write access to files and folders to help prevent virus/malware from modifying files
- Assessing clients on your network for vulnerabilities that make it prone to the current outbreak
- Deploying the latest components such as the virus pattern file and virus cleanup engine
- Performing a **Cleanup** on all the clients affected by the outbreak
- If enabled, scanning your clients and networks and takes action against detected threats

Outbreak Defense Details

Navigation Path: Live Status > Threat Status > Outbreak Defense > More Info...

This page displays complete information about any ongoing outbreaks.

Automatic Outbreak Defense Detail

The Automatic Outbreak Defense Detail section displays information about the virus/malware that is currently on the Internet and could potentially affect your network and clients. Based on threat information, the Outbreak Prevention Policy (OPP) takes steps to protect the network and clients while Trend Micro develops a solution (See *Trend Micro Outbreak Prevention Policy* on page B-2).

This section provides the following information:

- **Alert Type:** Red or Yellow
- **Risk Level:** The level of risk the threat poses to clients and networks based on the number and severity of the virus/malware incident.
- **Delivery method:** How the threat is spread
- **Automatic Response:** Click to enable/disable the Automatic Response
- **Automatic Response Details:** Click **More info** to view the specific actions Outbreak Defense is using to protect your clients from the current threat.

Status of Desktops/Servers within Outbreak Prevention Enforcement

The section displays the total for the number of clients with and without automatic alert enabled. Click the number link under the **Enabled** and **Not Enabled** columns to view more information about specific clients.

Vulnerable Computers

The Vulnerable Computers section displays a list of clients that have vulnerabilities. A vulnerable computer has weaknesses in its operating system or applications. Many threats exploit these vulnerabilities to cause damage or gain unauthorized control. Therefore, vulnerabilities represent risks not only to each individual computer where they are located, but also to the other computers on your network.

Scan For Vulnerabilities Now

Clicking **Scan for Vulnerabilities Now** sends a notification to all the Security Agents to perform a vulnerability scan on the Clients. After clicking Scan for Vulnerabilities Now, The Scan Notifying Progress screen appears temporarily to show you the progress of the notification and then is replaced with the Scan Notifying Results screen.

The Scan Notifying Results screen displays whether or not the WFBS-SVC Server has successfully notified a Client. Unsuccessful results occur when a Client is offline or in unexpected situations such as when there are network interruptions.

Outbreak Alert Settings

Navigation Path: Live Status > Outbreak Defense > More Info... > Outbreak Alert Settings

Clicking this takes you to the **Administration > Global Settings** page. Here you can enable/disable red and yellow alerts issued by Trend Micro.

Red Alerts

Several infection reports from each business unit reporting rapidly spreading malware, where gateways and email servers may need to be patched.

The industry's first 45-minute Red Alert solution process is started: An official pattern release (OPR) is deployed with notification of its availability, any other relevant notifications are sent out, and fix tools and information regarding vulnerabilities are posted on the download pages.

Yellow Alerts

Infection reports are received from several business units as well as support calls confirming scattered instances. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download. In case of an email-spreading malware, content filtering rules, called Outbreak Prevention Policies (OPP), are sent out to automatically block related attachments on servers equipped with the product functionality.

Chapter 10

Managing Notifications

This chapter explains how to use the different notification options.

The topics discussed in this chapter include:

About Notifications

To minimize the amount of time Administrators need to monitor WFBS-SVC and to ensure Administrators receive early warnings via email about looming outbreak situations, set the WFBS-SVC Server to send notifications whenever there are abnormal events on the network.

The conditions for notifications also affect alert thresholds on the **Live Status** screen (see *Configuring Alert Thresholds* on page 3). The conditions trigger the status icon to change from Normal to Warning or to Action Required.

By default, all events listed on the Notifications screen are selected and trigger the WFBS-SVC Server to send a notification to the system Administrator.

Threat Events

- **Outbreak Defense:** An alert is declared by TrendLabs or highly critical vulnerabilities are detected.
- **Antivirus:** Virus/malware detected on clients exceed a certain number, actions taken against virus/malware are unsuccessful, Real-time Scan disabled on clients.
- **Anti-spyware:** Spyware/grayware detected on clients, including those that require restarting the infected client to completely remove the spyware/grayware threat. You can also configure the spyware/grayware notification threshold, that is, the number of spyware/grayware incidents detected within the specified time period (default is one hour).
- **Web Reputation:** The number of URL violations exceeds the configured number in a certain period.
- **URL Filtering:** The number of URL violations exceeds the configured number in a certain period.
- **Behavior Monitoring:** The number of policy violations exceeds the configured number in a certain period.
- **Network Virus:** Network viruses detected exceeds a certain number.

System Events

- **Smart Scan:** Clients configured for Smart Scan cannot connect to the Smart Scan server or the server is not available.
- **Component update:** Last time components updated exceeds a certain number of days or updated components not deployed to Agents quick enough.

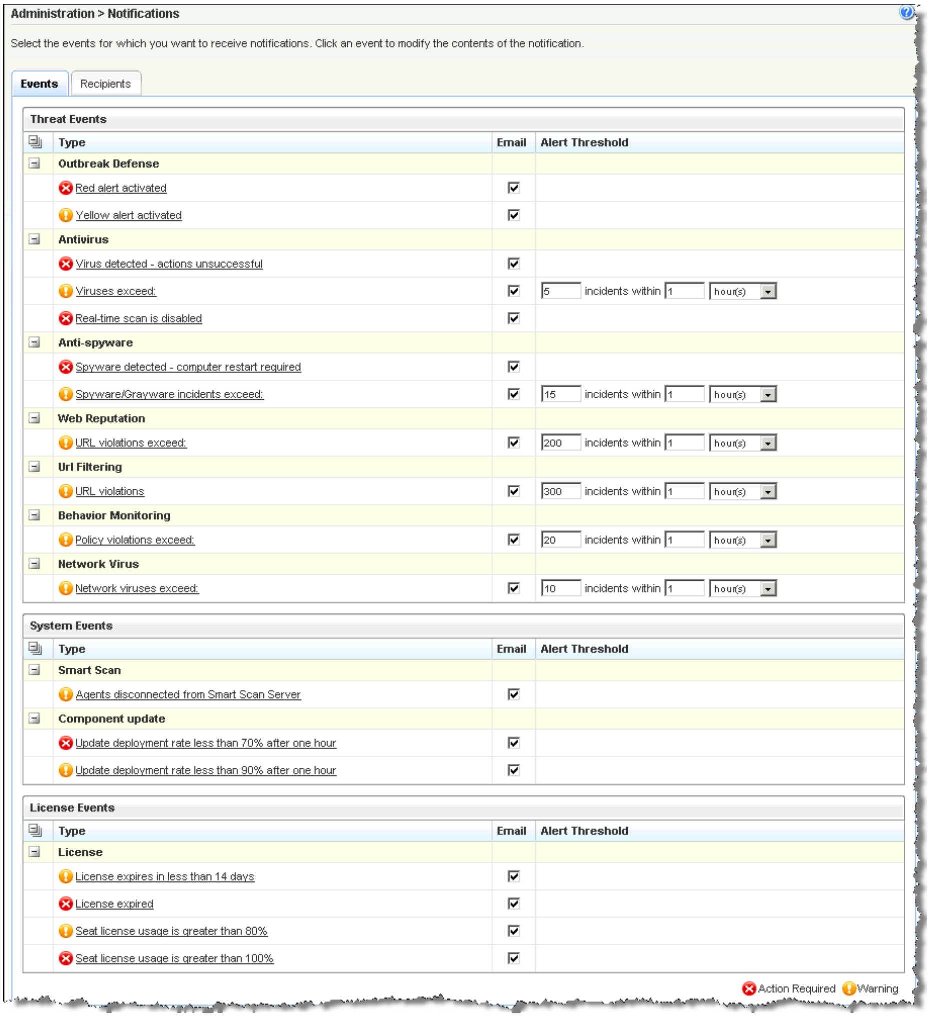
License Events

- **License is going to expire**
- **License expired**
- **Seat License usage is greater than 80%**
- **Seat License usage is greater than 100%**

Configuring Alert Thresholds

Navigation Path: Administration > Notifications > Events

Alert Thresholds affect both alerts on the Live Status screen and email alerts.



Administration > Notifications

Select the events for which you want to receive notifications. Click an event to modify the contents of the notification.

Threat Events

Type	Email	Alert Threshold
Outbreak Defense		
⊗ Red alert activated	☑	
⚠ Yellow alert activated	☑	
Antivirus		
⊗ Virus detected - actions unsuccessful	☑	
⚠ Viruses exceed:	☑	5 incidents within 1 hour(s) ▾
⊗ Real-time scan is disabled	☑	
Anti-spyware		
⊗ Spyware detected - computer restart required	☑	
⚠ Spyware/Grayware incidents exceed:	☑	15 incidents within 1 hour(s) ▾
Web Reputation		
⚠ URL violations exceed:	☑	200 incidents within 1 hour(s) ▾
Url Filtering		
⚠ URL violations	☑	300 incidents within 1 hour(s) ▾
Behavior Monitoring		
⚠ Policy violations exceed:	☑	20 incidents within 1 hour(s) ▾
Network Virus		
⚠ Network viruses exceed:	☑	10 incidents within 1 hour(s) ▾

System Events

Type	Email	Alert Threshold
Smart Scan		
⚠ Agents disconnected from Smart Scan Server	☑	
Component update		
⊗ Update deployment rate less than 70% after one hour	☑	
⚠ Update deployment rate less than 90% after one hour	☑	

License Events

Type	Email	Alert Threshold
License		
⚠ License expires in less than 14 days	☑	
⊗ License expired	☑	
⚠ Seat license usage is greater than 80%	☑	
⊗ Seat license usage is greater than 100%	☑	

⊗ Action Required ⚠ Warning

FIGURE 10-1. Notification Events screen

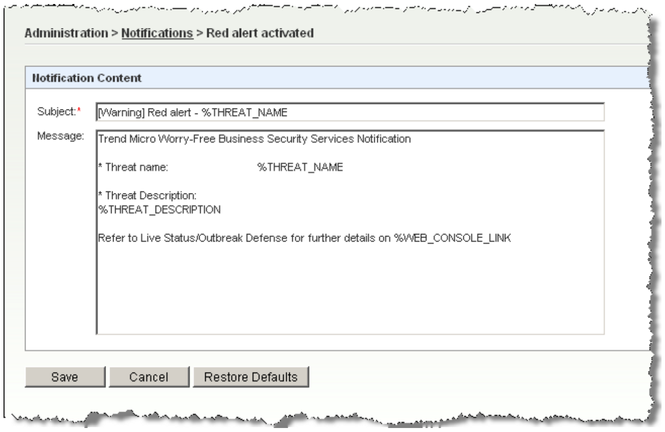
To configure notification events:

1. From the **Events** tab on the **Administration** screen, update the following as required (click ⊞ to expand each event):
   - **Email:** Select those events to which you would like to receive notifications. Alternatively, select check boxes corresponding to individual events.
   - **Alert Threshold:** Configure the number of incidents within each time period to trigger an alert.
2. Click **Save**.

Customizing Notification Alerts

Navigation Path: Administration > Notifications > Events > {notification link}

You can customize the subject line and the message body of each event notification.



Administration > Notifications > Red alert activated

Notification Content

Subject:* [Warning] Red alert - %THREAT_NAME

Message:

Trend Micro Worry-Free Business Security Services Notification

* Threat name: %THREAT_NAME

* Threat Description:
%THREAT_DESCRIPTION

Refer to Live Status/Outbreak Defense for further details on %WEB_CONSOLE_LINK

FIGURE 10-2. (Red Alert) Notification content screen

To customize the content of a notification:

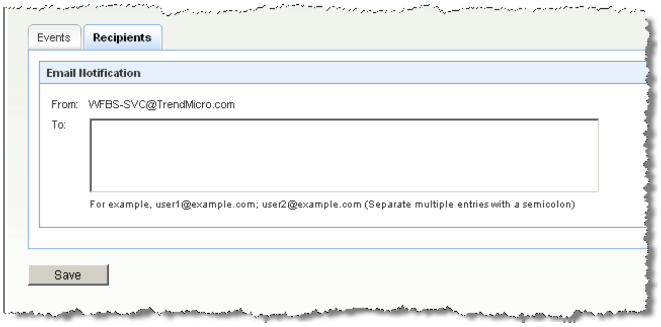
WARNING! Do not change the information enclosed in square brackets.

---

1. Click the event you wish to customize.
2. Edit as desired.
3. Click **Save**.

Configuring Notification Settings

Navigation Path: Administration > Notifications > Recipients



Email Notification

From: WFBS-SVC@TrendMicro.com

To:

For example, user1@example.com; user2@example.com (Separate multiple entries with a semicolon)

FIGURE 10-3. Notifications screen

Notification settings consist of setting only the To fields. Separate multiple email addresses in the To field with semicolons.

Chapter 11

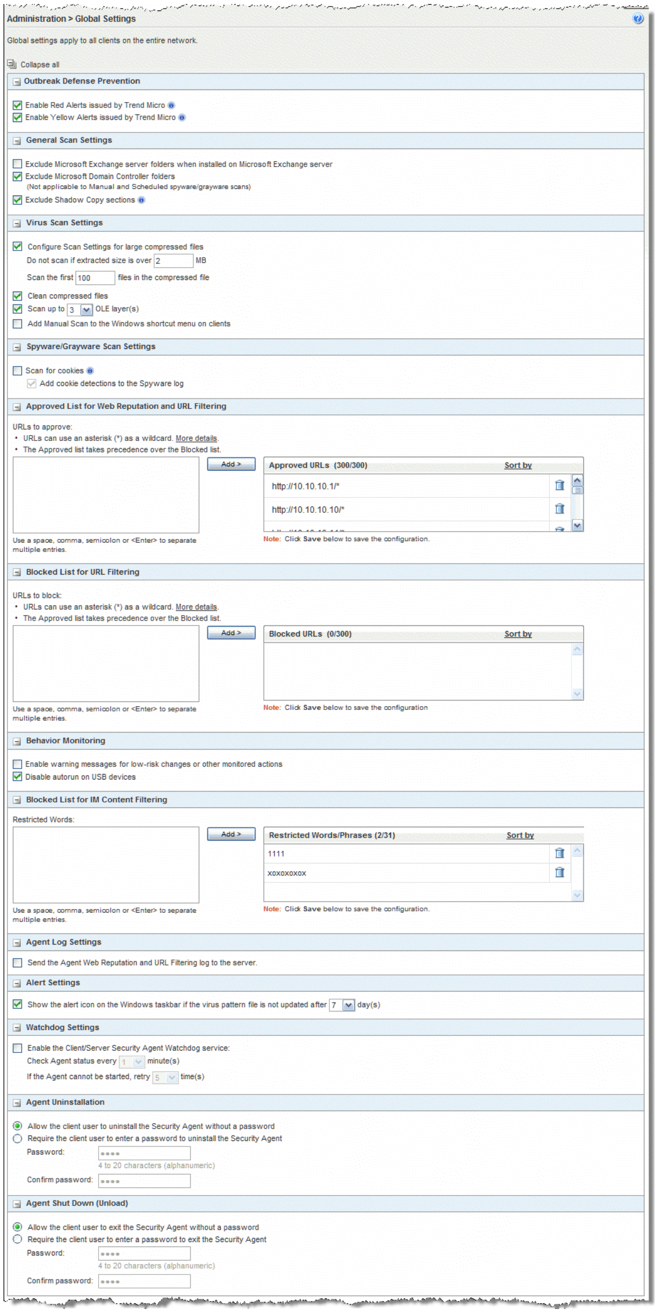
Configuring Global Settings

From the Web console, you can configure global settings for the WFBS-SVC Server and for desktops and servers protected by Client/Server Security Agents.

Global Settings

Navigation Path: Administration > Global Settings

WFBS-SVC global settings are configured here.



Administration > Global Settings

Global settings apply to all clients on the entire network.

Collapse all

Outbreak Defense Prevention

☑ Enable Red Alerts issued by Trend Micro
☑ Enable Yellow Alerts issued by Trend Micro

General Scan Settings

☐ Exclude Microsoft Exchange server folders when installed on Microsoft Exchange server
☑ Exclude Microsoft Domain Controller folders
(Not applicable to Manual and Scheduled spyware/grayware scans)
☑ Exclude Shadow Copy sections

Virus Scan Settings

☑ Configure Scan Settings for large compressed files
Do not scan if extracted size is over 2 MB
Scan the first 100 files in the compressed file
☑ Clean compressed files
☑ Scan up to 3 OLE layer(s)
☐ Add Manual Scan to the Windows shortcut menu on clients

Spyware/Grayware Scan Settings

☐ Scan for cookies
☑ Add cookie detections to the Spyware log

Approved List for Web Reputation and URL Filtering

URLs to approve:
- URLs can use an asterisk (*) as a wildcard. More details.
- The Approved list takes precedence over the Blocked list.

Add >

Approved URLs (300/300)	Sort by
http://10.10.10.1/*	
http://10.10.10.10/*	

Use a space, comma, semicolon or <Enter> to separate multiple entries.

Note: Click **Save** below to save the configuration.

Blocked List for URL Filtering

URLs to block:
- URLs can use an asterisk (*) as a wildcard. More details.
- The Approved list takes precedence over the Blocked list.

Add >

Blocked URLs (0/300)	Sort by

Use a space, comma, semicolon or <Enter> to separate multiple entries.

Note: Click **Save** below to save the configuration

Behavior Monitoring

☐ Enable warning messages for low-risk changes or other monitored actions
☑ Disable autorun on USB devices

Blocked List for IM Content Filtering

Restricted Words:

Add >

Restricted Words/Phrases (2/31)	Sort by
1111	
xoxoxoxox	

Use a space, comma, semicolon or <Enter> to separate multiple entries.

Note: Click **Save** below to save the configuration.

Agent Log Settings

☐ Send the Agent Web Reputation and URL Filtering log to the server.

Alert Settings

☑ Show the alert icon on the Windows taskbar if the virus pattern file is not updated after 7 day(s)

Watchdog Settings

☐ Enable the Client/Server Security Agent Watchdog service:
Check Agent status every 1 minute(s)
If the Agent cannot be started, retry 5 time(s)

Agent Uninstallation

● Allow the client user to uninstall the Security Agent without a password
○ Require the client user to enter a password to uninstall the Security Agent
Password: ••••
4 to 20 characters (alphanumeric)
Confirm password: ••••

Agent Shut Down (Unload)

● Allow the client user to exit the Security Agent without a password
○ Require the client user to enter a password to exit the Security Agent
Password: ••••
4 to 20 characters (alphanumeric)
Confirm password: ••••

FIGURE 11-1. Administration tab of the Global Settings screen

To set Global Settings:

1. From the **Global Settings** screen, update the following as required:
   - *Outbreak Defense Prevention* on page 11-3
   - *General Scan Settings* on page 11-3
   - *Virus Scan Settings* on page 11-3
   - *Spyware/Grayware Scan Settings* on page 11-4
   - *URL Filtering and Web Reputation* on page 11-4
   - *Behavior Monitoring* on page 11-5
   - *IM Content Filtering* on page 11-5
   - *Alert Settings* on page 11-5
   - *Watchdog Settings* on page 11-5
   - *Agent Uninstallation* on page 11-6
   - *Agent Shut Down (Unload)* on page 11-6
2. Click **Save**.

Outbreak Defense Prevention

Although they can be turned off, the following should remain enabled at all times to take advantage of Outbreak Prevention.

- **Enable Red Alerts issued by Trend Micro**
- **Enable Yellow Alerts issued by Trend Micro**

General Scan Settings

From the **Global Settings** screen, update the following as required:

- **Exclude Microsoft Exchange server folders when installed on Microsoft Exchange server:** Prevents Agents installed on the Microsoft Exchange server from scanning Microsoft Exchange folders.
- **Exclude Microsoft Domain Controller folders** (Not applicable to Manual and Scheduled spyware/grayware scans)**:** Prevents Agents installed on the Domain Controller from scanning Domain Controller folders. These folders store user information, user names, passwords, and other information.
- **Exclude Shadow Copy sections:** Shadow Copy or Volume Snapshot Services takes manual or automatic backup copies or snapshots of a file or folder on a specific volume.

Virus Scan Settings

From the **Global Settings** screen, update the following as required:

- **Configure scan settings for large compressed files:** Specify the maximum size of the extracted file and the number of files in the compressed file the Agent should scan.
- **Clean compressed files:** Agents will try to clean infected files within a compressed file.
- **Scan the OLE layers of compressed files:** Agents will scan the specified number of Object Linking and Embedding (OLE) layers. OLE allows users to create objects with one application and then link or embed them in a second application. For example, an .xls file embedded in a .doc file.
- **Add Manual Scan to the Windows shortcut menu on clients:** Adds a **Scan with Client/Server Security Agent** link to the context-sensitive menu. With this, users can right-click a file or folder (on the Desktop or in Windows Explorer) and manually scan the file or folder.

Spyware/Grayware Scan Settings

From the **Global Settings** screen, update the following as required:

- **Scan for cookies:** Agents will scan for and remove tracking cookies downloaded to clients by visiting Web sites. Detected tracking cookies are added to the spyware/grayware counter on the **Live Status** screen.
- **Add cookie detections to the Spyware log:** Adds each detected spyware cookie to the spyware log.

URL Filtering and Web Reputation

The Approved and Blocked lists allow you to over-ride the defined categories of URL Filtering (see *URL Filtering* on page 7-9) and Web Reputation (see *Web Reputation* on page 7-8).

The Blocked list is only supported by URL Filtering

The Approved list is supported by both URL Filtering and Web Reputation.

From the **Global Settings** screen, update the following as required:

- **URLs to approve:** Separate multiple URLs with a space, comma (,), semicolon (;) or <enter>. Click **Add**..
- **URLs to block:** Separate multiple URLs with a space, comma (,), semicolon (;) or <enter>. Click **Add**.

Note: Approving or blocking a URL implies approving or blocking all of its sub domains.

Note: The Blocked list is only supported by URL Filtering.
The Approved list is supported by both URL Filtering and Web Reputation.

When adding URLs to the lists, keep the following in mind:

- URLs can use an asterisk (*) as a wildcard (The asterisk matches zero or more characters).
- The Approved list takes precedence over the Blocked list.
- "http://" or "https://" must precede the URL.

The following URLs using the wildcard are acceptable:

- http://www.example.com/*
- http://*.example.com

The following URLs ending with a wildcard are not acceptable:

- http://www.example.com*
- http://www.example.*
- http://www.example.com.tw.*
- http://*.example.*

The following URLs with the wildcard as the last character in the host name are not acceptable:

- http://www.example.*/test/abc.html would become http://www.example.*/*
- http://www.example.com*/123/ would become http://www.example.com*/*

Filtering only supports the FQDN, not the path. For example:

- http://www.example.com/hu* would become http://www.example.com/*
- http://www.ex*le.com/abc/*.* would become http://www.ex*le.com/*

To delete an entry, click the corresponding trash can icon.

To edit an existing URL, click the URL.

To sort URLs, click the **Sort By** drop-down.

Send the Agent Web Reputation and URL Filtering log to the server: Agents will send details of accessed URLs to the WFBS-SVC Server.

Behavior Monitoring

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

- **Enable warning messages for low-risk changes or other monitored actions:** Agents warn users of low-risk changes or monitored actions.
- **Disable autorun when a USB device is plugged in.**

IM Content Filtering

Administrators can restrict the usage of certain words or phrases in instant messaging applications.

Agents can restrict words used in the following IM applications:

- America Online® Instant Messenger (AIM) 6 (builds released after March 2008 are not supported)
- ICQ® 6 (builds released after March 2008 are not supported)
- MSN™ Messenger 7.5, 8.1
- Windows Messenger Live™ 8.1, 8.5
- Yahoo!™ Messenger 8.1

From the **Administration** tab of the **Global Settings** screen, use the following fields as described:

- **Restricted Words:** Use this field to add restricted words or phrases. You are restricted to a maximum of 31 words or phrases. Each word or phrase cannot exceed 35 characters (17 for Chinese characters). Type an entry or multiple entries separated by semicolons (;) and then click **Add**>.
- **Restricted Words/Phrases** list**:** Words or phrases in this list cannot be used in IM conversations. To delete an entry, click the corresponding trash can icon.

Alert Settings

From the **Global Settings** screen, update the following as required:

- **Show the alert icon on the Windows taskbar if the virus pattern file is not updated after { } days:** Displays an alert icon on clients when the pattern file is not updated after a certain number of days.

Watchdog Settings

The Watchdog option ensures the Client/Server Security Agent is constantly protecting clients. When enabled, the Watchdog checks the availability of the Agent every x minutes. If the Agent is unavailable, the Watchdog will attempt to restart the Agent.

Tip: Trend Micro recommends enabling the Watchdog service to help ensure that the Client/Server Security Agent is protecting your clients. If the Client/Server Security Agent unexpectedly terminates, which could happen if the client is under attack from a hacker, the Watchdog service restarts the Client/Server Security Agent.

From the **Administration** tab of the **Global Settings** screen, update the following as required:

- Enable the Agent Watchdog service
- **Check client status every {} minutes:** Determines how often the Watchdog service should check client status.
- **If the client cannot be started, retry {} times**: Determines how many times the Watchdog service should attempt to restart the Client/Server Security Agent.

Agent Uninstallation

From the **Administration** tab of the **Global Settings** screen, update the following as required:

- **Allow the client user to uninstall the Security Agent without a password:** Allows users to uninstall the Security Agent.
- **Require the client users to enter a password to uninstall the Security Agent:** Allows users to uninstall the Security Agent after providing the specified password.

Agent Shut Down (Unload)

From the **Administration** tab of the **Global Settings** screen, update the following as required:

- **Allow the client user to exit the Security Agent without a password:** Allows users to exit the Security Agent.
- **Require the client users to enter a password to exit the Security Agent:** Allows users to exit the Security Agent after providing the specified password.

Chapter 12

Managing Updates

This chapter explains how to use and configure updates.

The topics discussed in this chapter include:

- *About Updates* on page 12-2
- *About ActiveUpdate* on page 12-2
- *Updatable Components* on page 12-3
- *Manual Updates* on page 12-4

About Updates

WFBS-SVC makes upgrading to the latest components easy by having the Active Agent automatically receive updated components from the Trend Micro Active Update Server. Then, all Inactive Agents receive updates from the Active Agent. By default, Agents are updated every two hours.

Agents not connected to the LAN will receive updates from Trend Micro Active Update instead of from the Active Agent.

Trend Micro recommended settings for component updates provide reasonable protection to small and medium-sized business. If necessary, you can run Manual updates at any time for all computers in a group by clicking **Computers >** {group} **> Others > Update Now**.

Inactive Agents

All the Worry-Free Business Security Services Agents, other than the Active Agent, are known as Inactive Agents. Inactive Agents are updated by the Active Agent.

Active Agent

The Active Agent serves as the contact window between the WFBS-SVC server and all WFBS-SVC Agents in a company.

It is responsible for:

- Communicating with the WFBS-SVC server
- Distributing updates and pattern files to other clients

The Active Agent periodically checks the Trend Micro ActiveUpdate (TMAU) Server for component and pattern file updates. If there are updates, the Active Agent downloads the update and notifies Inactive Agents about the update. Inactive Agents are then given a random time between 0 seconds to 15 minutes to download the update from the Active Agent. This prevents excessive utilization of the Active Agent's system resources.

Using the Active Agent election algorithm, WFBS-SVC Agents in a company elect one Agent to be the Active Agent. If the computer hosting the current Active Agent becomes unavailable, all other Agents immediately elect a new Active Agent.

About ActiveUpdate

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides the latest downloads of virus pattern files, scan engines, and program files through the Internet. ActiveUpdate does not interrupt network services or require you to restart clients.

One Agent, the Active Agent, in a network will receive updates from the ActiveUpdate Server. All other Agents (called Inactive Agents) in the network will receive updates from the Active Agent.

Incremental updates of the pattern files

ActiveUpdate supports incremental updates of pattern files. Rather than downloading the entire pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce bandwidth needed to update your antivirus software.

Updatable Components

To ensure clients stay protected from the latest threats, be sure the Client/Server Security Agents are up to date with the latest components.

WFBS-SVC components are updated automatically or can be manually updated. See *Manual Updates* on page 12-4.

TABLE 12-1. Updatable Components

COMPONENT	SUB-COMPONENT
Antivirus	Virus pattern Virus scan engine 32-bit Virus scan engine 64-bit Virus cleanup template Virus cleanup engine 32-bit Virus cleanup engine 64-bit IntelliTrap Exception Pattern IntelliTrap Pattern Feedback engine 32-bit Feedback engine 64-bit Smart Scan Pattern Smart Scan Agent Pattern
Anti-spyware	Spyware scan engine 32-bit Spyware scan engine 64-bit Spyware pattern Spyware active-monitoring pattern
Web Reputation	URL filtering engine 32-bit URL filtering engine 64-bit
Behavior Monitoring	Behavior Monitoring Driver Behavior Monitoring Core Service Policy Enforcement Pattern Digital Signature Pattern Behavior Monitoring Configuration Pattern Behavior Monitoring Detection Pattern
Outbreak Defense	Vulnerability pattern
Network Virus	Common firewall pattern Common firewall engine 32-bit Common firewall engine 64-bit Transport Driver Interface (TDI) driver 32-bit Transport Driver Interface (TDI) driver 64-bit WFP driver 32-bit WFP driver 64-bit

See *Components* on page 1-8 for detailed information about each component.

Default Update Times

By default, the Active Agent in a network checks for updates and downloads components, if necessary, from the Trend Micro ActiveUpdate Server under the following circumstances:

- When you install the product for the first time, all components for the Agents are immediately updated.
- Client/Server Security Agent runs a scheduled update every 2 hours.

The Trend Micro recommended settings for component updates provide reasonable protection to small- and medium-sized business. If necessary, you can run Manual updates.

Generally, Trend Micro updates the scan engine or program only during the release of a new WFBS-SVC version. However, Trend Micro releases pattern files frequently.

Manual Updates

Navigation Path: Computers > {group} **> Others > Update Now**

The Active Agent periodically checks commands from the WFBS-SVC. If they include **Update Now**, the Active Agent downloads the update from Trend Micro Active Update, and then notifies Inactive Agents to update.

Chapter 13

Using Logs and Reports

This chapter describes how to use logs and reports to monitor your system and analyze your protection.

The topics discussed in this chapter include:

Reports

Worry-Free Business Security Services allows you to create and view reports that contain detailed information about detected threats. Reports also include ranking to identify the most vulnerable computers. WFBS-SVC generates reports in .pdf format.

You can generate a log query from the **Reports** screen. A log query displays information about the virus/malware, spyware/grayware, or malicious URLs detected on your network for the specified time. It also provides detailed information about the names of the affected computers, threats, and affected files. It also lists the scan type and action taken on that particular threat.

From the **Reports** screen, you can:

- Create a new report
- Delete an existing report
- Generate a log query

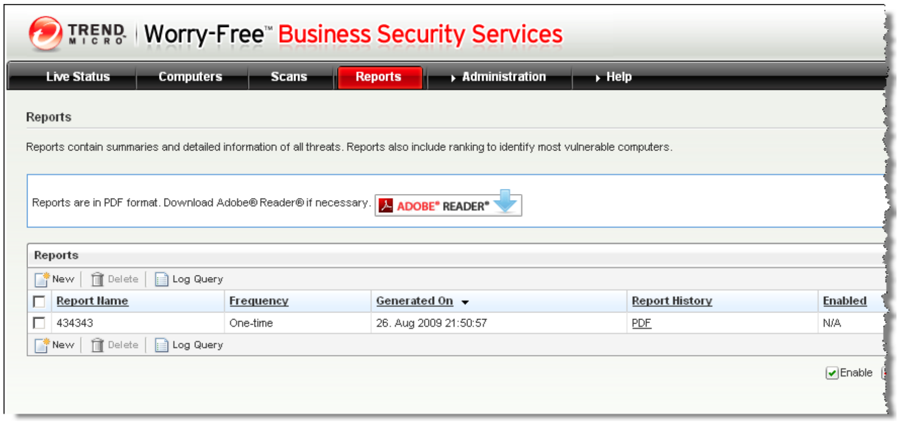
You can create reports for a specific time period or time zone depending on your needs. The reports contain the following information:

- Time, date, and time zone for which the report is generated.
- **Virus/Malware Summary**. Represents the information about the activities, number of incidents, and percentage of the virus/malware. It ranks the virus/malware based on number of incidents and percentage. It also displays a graphical representation of the activities.

Generating Reports

Navigation Path: Reports > New

One-time reports provide a summary just once. Scheduled reports provide a summary on a regular basis.



Reports

Reports contain summaries and detailed information of all threats. Reports also include ranking to identify most vulnerable computers.

Reports are in PDF format. Download Adobe® Reader® if necessary.

Reports

□	Report Name	Frequency	Generated On	Report History	Enabled
□	434343	One-time	26. Aug 2009 21:50:57	PDF	N/A

FIGURE 13-1. Reports screen

To create or schedule a report:

1. From the **Reports** screen, click **New**.
2. Update the following as required:
   - **Report Name**
   - **Schedule:** Applicable only for Scheduled Reports.
     - **One-time:** Creates the report one time.
     - **Weekly, every:** The Report runs once a week on the specified day at the specified time.

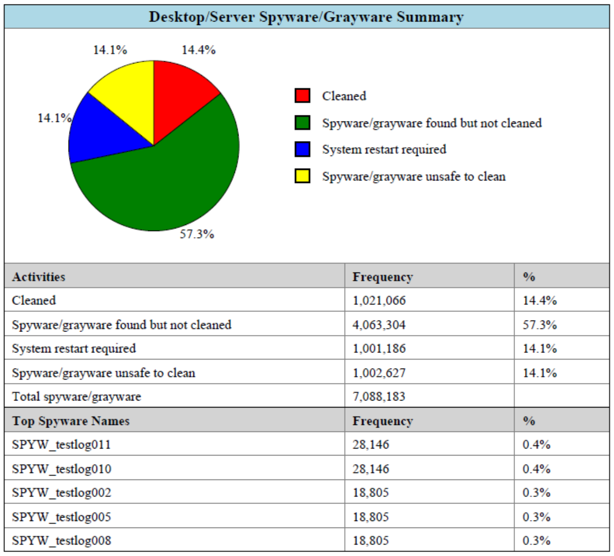
- **Monthly, on day:** The Report runs once a month on the specified day at the specified time. If you select 31 days and the month has only 30 days, WFBS-SVC will not generate the report that month.
- **Generate report at:** The time WFBS-SVC should generate the report.

- **Send the report to:** WFBS-SVC sends the generated report to the specified recipients. Separate multiple entries with semicolons (;).

3. Click **Generate**. View the report from the **Reports** screen by clicking either **PDF** or the number of the reports that have been generated under the Report History column. If you click a number, a subscreen will open where you can view a specific report.

   To delete a report, from the **One-Time Reports or Scheduled Reports** screen, select the check box corresponding to the report and click **Delete.**

   To edit a scheduled report, click the name of the report on the **Reports** screen and update the options as required.


Desktop/Server Spyware/Grayware Summary
14.1%
14.4%
14.1%
57.3%
🟥 Cleaned
🟩 Spyware/grayware found but not cleaned
🟦 System restart required
🟨 Spyware/grayware unsafe to clean

Activities	Frequency	%
Cleaned	1,021,066	14.4%
Spyware/grayware found but not cleaned	4,063,304	57.3%
System restart required	1,001,186	14.1%
Spyware/grayware unsafe to clean	1,002,627	14.1%
Total spyware/grayware	7,088,183	
Top Spyware Names	**Frequency**	**%**
SPYW_testlog011	28,146	0.4%
SPYW_testlog010	28,146	0.4%
SPYW_testlog002	18,805	0.3%
SPYW_testlog005	18,805	0.3%
SPYW_testlog008	18,805	0.3%

FIGURE 13-2. Sample report showing Spyware/grayware Summary

Editing Reports

Navigation Path: Reports > {Report Name}

Edit reports by clicking on the report name on the **Reports** screen.

To edit report:

1. From the **Reports** screen, click the report name.
2. Update the following as required:
   - **Report Name**
   - **Schedule:** Applicable only for Scheduled Reports.
     - **One-time:** Creates the report one time.
     - **Weekly, every:** The Report runs once a week on the specified day at the specified time.

    - **Monthly, on day:** The Report runs once a month on the specified day at the specified time. If you select 31 days and the month has only 30 days, WFBS-SVC will not generate the report that month.
    - **Generate report at:** The time WFBS-SVC should generate the report.
  - **Send the report to:** WFBS-SVC sends the generated report to the specified recipients. Separate multiple entries with semicolons (;).

3. Click **Save**.

   To edit a scheduled report, click the name of the report on the **Reports** screen and update the options as required.

Interpreting Reports

WFBS-SVC reports contain the following information.

TABLE 13-1. Contents of a Report

REPORT ITEM	DESCRIPTION
Antivirus	**Desktop/Server Virus Summary** Virus reports show detailed information about the numbers and types of virus/malware that the scan engine detected and the actions it took against them. The report also lists the Top virus/malware names. Click the names of the virus/malware to open a new Web browser page and redirect it to the Trend Micro virus encyclopedia to learn more about that virus/malware.
Anti-spyware	**Desktop/Servers Spyware/Grayware Summary** The spyware/grayware report shows detailed information about the spyware/grayware threats detected on clients, including the number of detections and the actions that WFBS-SVC took against them. The report includes a pie chart that shows the percentage of each anti-spyware scan action that has been performed.
Antivirus	**Top 5 Desktop/Servers with Virus Detections** Displays the top five desktops or servers reporting virus/malware detections. Observing frequent virus/malware incidents on the same client might indicate that a client represents a high security risk that might require further investigation
Network Virus	**Top 10 Network Viruses Detected** Lists the 10 network viruses most frequently detected by the common firewall driver. Click the names of the viruses to open a new Web browser page and redirect it to the Trend Micro virus encyclopedia to learn more about that virus. **Top 10 Computers Attacked** List the computers on your network that report the most frequent virus incidents.
Anti-spyware	**Top 5 Desktop/Servers with Spyware/Grayware Detections** The report also shows the top five spyware/grayware threats detected and the five desktops/servers with the highest number of spyware/grayware detected. To learn more about the spyware/grayware threats that have been detected, click the spyware/grayware names. A new Web browser page opens and displays related information on the spyware/grayware on the Trend Micro Web site.
Web Reputation	**Top 10 Computers Violating Web Threat Protection Policies** Lists the top 10 clients that have violated Web Threat Protection policies.

TABLE 13-1. Contents of a Report

REPORT ITEM	DESCRIPTION
URL Filtering	**Top 5 URL Category Policies Violated** Lists the most commonly accessed Web site categories that violated the policy. **Top 10 Computers Violating URL Category Policies** Lists the top 10 clients that have violated URL Category policies.
Behavior Monitoring	**Top 5 Programs Violating Behavior Monitoring Policies** Lists the top five programs violating Behavior Monitoring policies. **Top 10 Computers Violating Behavior Monitoring Policies** Lists the top 10 clients that have violated Behavior Monitoring policies.

Deleting Reports

To delete an existing report:

1. From the Web console, click **Reports**.
2. On the **Reports** screen, select the reports you want to delete.
3. Click **Delete**.

WARNING! **Deleted reports cannot be recovered. Trend Micro recommends downloading reports before deleting them.**

Logs

WFBS-SVC keeps comprehensive logs about virus/malware and spyware/grayware incidents, events, and updates. Use these logs to assess your organization's protection policies and to identify clients that are at a higher risk of infection. Also, use these logs to verify that updates have been deployed successfully.

Note: Use spreadsheet applications, such as Microsoft Excel, to view CSV log files.

WFBS-SVC maintains logs under the following categories:

- Management console event logs
- Desktop/Server logs

TABLE 13-2. Log Type and Content

TYPE (EVENT OR ITEM THAT GENERATED THE LOG ENTRY)	CONTENT (TYPE OF LOG TO OBTAIN CONTENT FROM)
Management console events	Manual Scan Outbreak Defense events

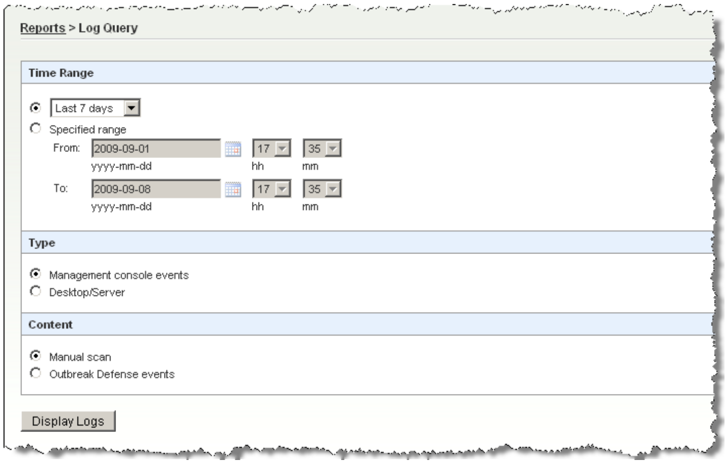
TABLE 13-2. Log Type and Content (Continued)

TYPE (EVENT OR ITEM THAT GENERATED THE LOG ENTRY)	CONTENT (TYPE OF LOG TO OBTAIN CONTENT FROM)
Desktop/Server	Virus logs • Real-time Scan • Manual Scan • Scheduled scan • Cleanup Spyware/Grayware logs • Real-time Scan • Manual Scan • Scheduled scan Web Reputation logs URL Filtering logs Behavior monitoring logs Update logs Network virus logs Outbreak Defense logs Event logs

Using Log Query

Navigation Path: Reports > Log Query

Perform log queries to gather information from the log database. You can use the **Log Query** screen to set up and run your queries. Results can be exported in the CSV file format or printed.



Reports > Log Query

Time Range

● Last 7 days
○ Specified range
From: 2009-09-01 yyyy-mm-dd 17 hh 35 mm
To: 2009-09-08 yyyy-mm-dd 17 hh 35 mm

Type

● Management console events
○ Desktop/Server

Content

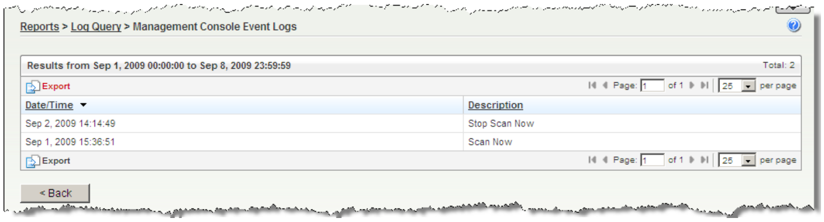
● Manual scan
○ Outbreak Defense events

FIGURE 13-3. Default Log Query screen

To view logs:

1. From the **Log Query** screen, update the following options as required:
   - **Time Range**
     - **Preconfigured range**
     - **Specified range:** To limit the query to certain dates.
   - **Type:** See Table 13-2 on page 13-5 to view the contents of each log type.
     - **Management console events**
     - **Desktop/Server**
   - **Content:**
     - Virus logs
     - Spyware/grayware logs
     - Web Reputation logs
     - URL Filtering logs
     - Behavior Monitoring logs
     - Update logs
     - Network virus logs
     - Outbreak Defense events
     - Event logs
2. Click **Display Logs**.

   To save the log as a comma-separated value (CSV) data file, click **Export**. Use a spreadsheet application to view CSV files.



Reports > Log Query > Management Console Event Logs

Results from Sep 1, 2009 00:00:00 to Sep 8, 2009 23:59:59 Total: 2

Date/Time ▼	Description
Sep 2, 2009 14:14:49	Stop Scan Now
Sep 1, 2009 15:36:51	Scan Now

FIGURE 13-4. Sample Log Query screen

Chapter 14

Administering WFBS-SVC

This chapter explains how to use additional administrative tasks such as viewing the product license and working with client tools.

The topics discussed in this chapter include:

Client Tools

Navigation Path: Administration > Tools

This section contains information about WFBS-SVC Client tools.

Example Deployment Script

Navigation Path: Administration > Tools > Example Deployment Script

Download an example deployment script from here. See *Agent Installation - Additional Options* on page 3-6 for more information about deployment scripts for installing the Agent.

Restore Encrypted Virus

Navigation Path: Administration > Tools > Restore Encrypted Virus

Client/Server Security Agents encrypt infected files and attachments to prevent users from opening them and spreading virus/malware to other files on the client.

Whenever Client/Server Security Agent backs up, quarantines, or renames an infected file, it encrypts the file. The quarantined file is typically stored in the `C:\Program Files\Trend Micro\Client Server Security Agent\Suspect` folder on the client. A backup file is stored in the `\Backup` folder of the client in `C:\Program Files\Trend Micro\Client Server Security Agent\Backup\`.

There may be some situations when you have to open the file even if you know it is infected. For example, if an important document has been infected and you need to retrieve the information from the document, you will need to decrypt the infected file to retrieve your information. You use the Restore Encrypted Virus tool to decrypt infected files you want to open.

To prevent Client/Server Security Agent from detecting the virus/malware again when you use Restore Encrypted Virus, you also need to exclude the folder to which you decrypt the file from Real-time Scan. To do this:

1. Download the tool from the WFBS-SVC console from **Administration > Tools > Restore Encrypted Virus**

   Restore Encrypted Virus requires the following files:

   - **Main file:** VSEncode.exe
   - **Required DLL file:** VSAPI32.dll

2. Grant privileges to the client on the WFBS-SVC console. To do this:

   a. Click **Computers >** {group} **> Configure > Client Privileges > Antivirus/Anti-spyware**.

   b. Check the **Real -time Scan Settings** check box.

3. Exclude the directory on the client computer Agent application that will contain the decrypted file.

   a. Right click the Agent icon on the task bar.

   b. Click **Client/Server Security Agent Console** to open the Agent interface.

   c. Click **Scan > Scan Settings > Real Time Scan > Files to Scan**.

   d. Click the **Enable scan exclusion** check box.

   e. Click the **Edit** button. Add the directory (or files) you wish to open.

WARNING! Decrypting an infected file could spread the virus/malware to other files.

To restore files in the Suspect folder using the graphical interface:

1. Go to the folder where the tool is located (for example: c:\VSEncrypt) and enter VSEncode.exe /u.
2. Select the file to restore.
3. Click **Restore**.

To restore files in the Suspect folder from the command line:

1. Copy VSEncrypt from the Security Server to the client:

   \PCCSRV\Admin\Utility\VSEncrypt.

WARNING! **Do not copy the** VSEncrypt **folder to the** `..\Client Server Security Agent` **folder. The** VSAPI32.dll **file of Restore Encrypted Virus will conflict with the original** VSAPI32.dll**.**

2. Open a command prompt and go to the location where you copied the VSEncrypt folder.
3. Run Restore Encrypted Virus using the following parameters:
   - **no parameter:** Encrypt files in the Quarantine folder
   - **-d:** Decrypt files in the Quarantine folder
   - **-debug:** Create debug log and output in the root folder of the client
   - **/o:** Overwrite encrypted or decrypted file if it already exists
   - **/f:** {filename}. Encrypt or decrypt a single file
   - **/nr:** Do not restore original file name

For example, you can type VSEncode [-d] [-debug] to decrypt files in the Quarantine folder and create a debug log. When you decrypt or encrypt a file, the decrypted or encrypted file is created in the same folder.

Note: You may not be able to encrypt or decrypt files that are locked.

Restore Encrypted Virus provides the following logs:

- VSEncrypt.log. Contains the encryption or decryption details. This file is created automatically in the temp folder for the user logged on the machine (normally, on the C: drive).
- VSEncDbg.log. Contains the debug details. This file is created automatically in the temp folder for the user logged on the machine (normally, on the C: drive) if you run VSEncode.exe with the -debug parameter.

To encrypt or decrypt files in other locations:

1. Create a text file and then type the full path of the files you want to encrypt or decrypt.

   For example, if you want to encrypt or decrypt files in C:\My Documents\Reports, type C:\My Documents\Reports\*.* in the text file. Then save the text file with an INI or TXT extension, for example, you can save it as ForEncryption.ini on the C: drive.
2. At a command prompt, run Restore Encrypted Virus by typing VSEncode.exe -d -i {location of the INI or TXT file}, where {location of the INI or TXT file} is the path and file name of the INI or TXT file you created (for example, C:\ForEncryption.ini).

Small Business Server Add-in

Navigation Path: Administration > Tools > Add-In Tools

Trend Micro SBS Dashboard Add-In tool will allow administrators to access the WFBS-SVC console directly from a Microsoft Small Business Server (SBS) Essentials 2011 Dashboard. To install this tool, click **Download** and follow the onscreen instructions.

After the initial login, the WFBS-SVC user name and password will automatically be entered using the last values entered.

Changing Your Password

To change your password to the WFBS-SVC console, you need to change your password on the Registration System.

To change your password:

1. Log on to the Registration System.

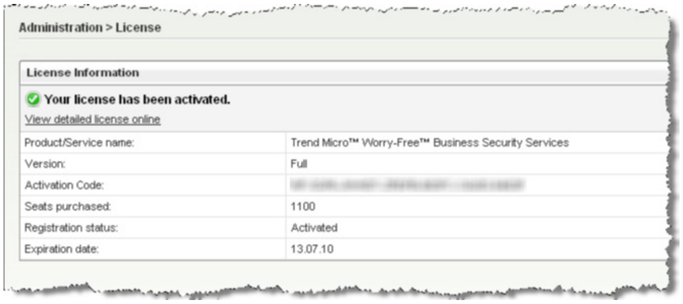
Note: Contact your sales representative for the URL.

2. Enter your existing Logon ID and password.
3. Click **My Company** in the left hand column.
4. Click the **Change Password** button and follow the onscreen instructions.

Viewing Product License Details

Navigation Path: Administration > Service License

From the service license screen, you can renew, upgrade, or view service license details.



Administration > License

License Information

✓ Your license has been activated.

View detailed license online

Product/Service name:	Trend Micro™ Worry-Free™ Business Security Services
Version:	Full
Activation Code:	[redacted]
Seats purchased:	1100
Registration status:	Activated
Expiration date:	13.07.10

FIGURE 14-1. Administration–Product License screen

The Service License screen displays details about your license. You might have a fully licensed version or an trial version. In either case, your license entitles you to a maintenance agreement. When your maintenance agreement expires, the clients on your network will be protected in a very limited way. Ensure that you renew your license before it expires.

Consequences of an Expired License

When a Full-version Activation Code expires, you can no longer perform important tasks, such as downloading updated components or using Web Reputation, etc.

To renew the product license:

1. Contact your sales representative or corporate reseller to renew your license agreement.
2. A Trend Micro representative will update your registration information using Trend Micro Product Registration.
3. You are not required to manually enter a new Activation Code when renewing your license.

Participating in Smart Protection Network

Navigation Path: Administration > Smart Protection Network

Trend Micro Smart Feedback continually gathers and analyzes threat information to help provide better protection. Your participation in Trend Micro Smart Feedback means that Trend Micro will gather information from your computer to help identify new threats. The information that Trend Micro collects from your computer is as follows:

- File checksums
- Web addresses accessed
- File information, including sizes and paths
- Names of executable files

Tip: You do not need to participate in Smart Feedback to protect your computers. Your participation is optional and you may opt out at any time. Trend Micro recommends that you participate in Smart Feedback to help provide better overall protection for all Trend Micro customers.

For more information on the Smart Protection Network, visit:

http://www.trendmicro.com/go/SmartProtectionNetwork

To enable Trend Micro Smart Feedback:

1. Click **Yes, I would like to join the Smart Protection Network**.
2. To send information about potential security threats in the files on your client computers, select the **File Feedback** check box.
3. To help Trend Micro understand your organization, choose the **Industry** type.
4. Click **Save**.

Worry-Free Remote Manager

The Trend Micro™ Worry-Free™ Remote Manager Agent allows resellers to manage WFBS-SVC remotely. See the WFRM documentation or talk to your reseller for details.

Appendix A

Client Information

This appendix explains the different types of clients and the client icons that appear in the system tray.

The topics discussed in this appendix include:

- *Normal Client Icons* on page A-2
- *32-bit and 64-bit Clients* on page A-5

Normal Client Icons

Conventional Scan Client Status: Normal

The following icons indicate that everything is normal with the clients configured for Conventional Scan.

TABLE A-1. Icons for Clients Under Normal Conditions (Conventional Scan)

Icon	Description
●	Normal client configured for Conventional Scan
◐	Conventional Scan is running

Conventional Scan Client Status: Clients Disconnected from the WFBS-SVC Server but Protected by Real-Time Scan

Clients can occasionally become disconnected from the WFBS-SVC Server. If you enabled Real-time Scan and the scan service is running normally, your clients will still be protected but could already have or soon have out-of-date pattern files. Clients with the icons below are still protected by Real-time Scan.

If the following icons appear, verify that your clients are connected to your network.

TABLE A-2. Icons for Clients Disconnected from the WFBS-SVC Server (Conventional Scan)

Icon	Description
●	Disconnected from the WFBS-SVC Server but Real-time Scan is running and the pattern file was up to date when the disconnection occurred
●!	Disconnected from the WFBS-SVC Server but Real-time Scan is running. However, the pattern file was not up to date when the disconnection occurred

Conventional Scan Client Status: Real-time Scan Not Operational

Trend Micro recommends enabling Real-time Scan. Although it can be disabled, it is not recommended. The following icons appear on clients when Real-time Scan is disabled.

TABLE A-3. Icons for Clients with Real-time Scan Disabled (Conventional Scan)

Icon	Description
⊘	Real-time Scan is disabled
⊘!	Real-time Scan is disabled and the pattern file is out of date
⊘	Real-time Scan is disabled and the client is disconnected from the WFBS-SVC Server
⊘!	Real-time Scan is disabled, the client is disconnected from the WFBS-SVC Server, and the pattern file is out of date

Clients with the following red icons are very vulnerable because the Real-time Scan service has been terminated or is not working properly.

TABLE A-4. Icons for Clients with Real-time Scan Not Working Properly (Conventional Scan)

Icon	Description
🔴	Real-time Scan Service is not running properly
🔴	Real-time Scan Service is not running properly and the pattern file is out of date
🔴	Real-time Scan Service is not running properly and the client is disconnected from the server
🔴	Real-time Scan Service is not running properly, the client is disconnected from the server, and the pattern file is out of date

Smart Scan Client Status: Normal

If the following icons appear, everything is normal with the clients configured for Smart Scan.

TABLE A-5. Icons for Clients Under Normal Conditions (Smart Scan)

Icon	Description
🔵	Normal client configured for Smart Scan
🔵	Smart Scan is running

Smart Scan Client Status: Disconnected from Smart Scan Server

Smart Scan technology relies on the Smart Scan server to protect your clients. If clients are configured for Smart Scan but disconnected from the Smart Scan Server, they will have only minimum level of protection. If the following icons appear, verify that the Smart Scan service `TMiCRCScanService` is running.

TABLE A-6. Icons for Clients with Real-time Scan Disabled (Smart Scan)

Icon	Description
🔵	Disconnected from the Scan Server but connected to the WFBS-SVC Server
🔵	Disconnected from the Scan Server and also disconnected from the WFBS-SVC Server

Smart Scan Client Status: Real-time Scan not Operational

Trend Micro recommends enabling Real-time Scan. Although it can be disabled, this is not recommended. The following icons appear on clients when Real-time Scan is disabled.

TABLE A-7. Icons for Clients with Real-time Scan Disabled (Smart Scan)

Icon	Description
🟩	Real-time Scan is disabled but the client is connected to the Scan Server and the WFBS-SVC Server
🟩	Real-time Scan is disabled, the client is connected to the Scan Server, but not the WFBS-SVC Server
🟥	Real-time Scan is disabled, the client is not connected to the Scan Server but is connected to the WFBS-SVC Server
🟥	Real-time Scan is disabled and the client is not connected to either the Scan Server or the WFBS-SVC Server

Clients with the following red icons are very vulnerable because the Real-time Scan service has been terminated or is not working properly.

TABLE A-8. Icons for Clients with Real-time Scan Not Working Properly (Smart Scan)

Icon	Description
🟩	Real-time Scan Service is not running properly, but the client is connected to the Scan Server and the WFBS-SVC Server
🟩	Real-time Scan Service is not running properly, the client is connected to the Scan Server but not the WFBS-SVC Server
🟥	Real-time Scan Service is not running properly, the client is not connected to the Scan Server but is connected to the WFBS-SVC Server
🟥	Real-time Scan Service is not running properly and the client is not connected to either the Scan Server or the WFBS-SVC Server

Invalid Company Key

When the license seat count is shown to be overused on the console (the seat count is full), but there are not as many Client/Server Security Agents in actual use, some clients may be using an invalid license. To recover the license seat count, the administrator needs to contact Trend Micro support and obtain a new Company Key. When a new Company Key has been set by Trend Micro, the Agents will be disconnected from the server, client protection will be disabled, and the system tray will show the Invalid Company Key icon. The new Company Key will need to be applied to all Client/Server Security Agents in the network.

TABLE A-9. Icon for an invalid Company Key.

Icon	Description
!	Invalid Company Key. Resetting the key is required.

To apply a new Company Key:

1. Click the Invalid Company Key icon on the system tray.
2. Enter the new Company Key from Trend Micro.
3. Click **Submit**.

32-bit and 64-bit Clients

The Agent supports computers that use x86 processor architecture and x64 processor architecture. All features are available for these operating systems and architectures except for Anti-Rootkit.

Note: The Agent does not support the Itanium™ 2 Architecture (IA-64).

Appendix B

Trend Micro Services

This appendix explains the services that Trend Micro offers.

The topics discussed in this appendix include:

- *Trend Micro Outbreak Prevention Policy* on page B-2
- *Trend Micro IntelliScan* on page B-2
- *Trend Micro ActiveAction* on page B-2
- *Trend Micro IntelliTrap* on page B-3
- *Trend Micro Web Reputation* on page B-4

Trend Micro Outbreak Prevention Policy

The Trend Micro Outbreak Prevention Policy is a set of Trend Micro recommended default security configuration settings that are applied in response to an outbreak on the network.

The Outbreak Prevention Policy is downloaded from Trend Micro to the WFBS-SVC Server.

When the WFBS-SVC Server detects an outbreak, it determines the degree of the outbreak and immediately implements the appropriate security measures as stated in the Outbreak Prevention Policy.

Based on the Outbreak Prevention Policy, Automatic Threat Response takes the following preemptive steps to secure your network in the event of an outbreak:

- Blocks shared folders to help prevent virus/malware from infecting files in shared folders
- Blocks ports to help prevent virus/malware from using vulnerable ports to infect files on the network and clients
- Denies write access to files and folders to help prevent virus/malware from modifying files
- Displays an alert message on clients when an outbreak detected

Trend Micro IntelliScan

IntelliScan is a new method of identifying files to scan. For executable files (for example, .exe), the true file type is determined based on the file content. For non-executable files (for example, .txt), the true file type is determined based on the file header.

Using IntelliScan provides the following benefits:

- **Performance optimization:** IntelliScan does not affect applications on the client because it uses minimal system resources
- **Shorter scanning period:** Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

Trend Micro ActiveAction

Different types of virus/malware require different scan actions. Customizing scan actions for different types of virus/malware requires knowledge about virus/malware and can be a tedious task. Trend Micro uses ActiveAction to counter these issues.

ActiveAction is a set of pre-configured scan actions for virus/malware and other types of threats. The recommended action for virus/malware is Clean, and the alternative action is Quarantine. The recommended action for Trojans and joke programs is Quarantine.

If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus/malware, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:

- **Time saving and easy to maintain:** ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- **Updatable scan actions:** Virus writers constantly change the way virus/malware attack computers. To help ensure that clients are protected against the latest threats and the latest methods of virus/malware attacks, new ActiveAction settings are updated in virus pattern files.

Default ActiveAction Settings

The default ActiveAction settings for the following threats are:

TABLE B-1. Default ActiveAction Settings

THREAT	ACTION	ACTION FOR UNCLEANABLE THREATS
Possible virus/malware	No action	Not Applicable
Joke	Quarantine	Not Applicable
Other Threats	Clean	Quarantine
Packer	Quarantine	Not Applicable
Test virus	Pass	Not Applicable
Virus	Clean	Quarantine
Worm/Trojans	Quarantine	Not Applicable

Note: Future pattern files could update the default actions.

Trend Micro IntelliTrap

IntelliTrap is a Trend Micro heuristic technology used to discover threats that use Real-Time Compression paired with other malware characteristics like packers. This covers virus/malware, worms, trojans, backdoors and bots. Virus writers often attempt to circumvent virus/malware filtering by using different file compression schemes. IntelliTrap is a real-time, rule-based, and pattern recognition scan engine technology that detects and removes known virus/malware in files compressed up to six layers deep using any of 16 popular compression types.

IntelliTrap uses the following components when checking for bots and other malicious programs:

- Trend Micro virus scan engine and pattern file
- IntelliTrap pattern and exception pattern

True File Type

When set to scan the "true file type", the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named "family.gif," it does not assume the file is a graphic file. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that someone named to avoid detection.

True file type scanning works in conjunction with IntelliScan to scan only those file types known to be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but with this reduction comes a potentially higher risk.

For example, .gif files make up a large volume of all Web traffic, but they are unlikely to harbor virus/malware, launch executable code, or carry out any known or theoretical exploits. Therefore, does this mean they are safe? Not entirely. It is possible for a malicious hacker to give a harmful file a "safe" file name to smuggle it past the scan engine and onto the network. This file could cause damage if someone renamed it and ran it.

Tip: For the highest level of security, Trend Micro recommends scanning all files.

Trend Micro 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.

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, see Configuring Global Settings.

Reputation Score

A URL's “reputation score” determines whether it is a Web threat or not. Trend Micro calculates the score using proprietary metrics. Trend Micro considers a URL “a Web threat”, “very likely to be a Web threat”, or “likely to be a Web threat” if its score falls within the range set for one of these categories.

Trend Micro considers a URL safe to access if its score exceeds a defined threshold. There are three security levels that determine whether CSA will allow or block access to a URL.

- **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

Appendix C

Best Practices for Protecting Your Clients

There are many steps you can take to protect your computers and network from Internet threats. Trend Micro recommends the following actions:

- Use the Trend Micro recommended WFBS-SVC default settings.
- Keep your operating systems and all software updated with the latest patches.
- Use strong passwords and advise your end users to use strong passwords.

  A strong password should be at least eight characters long and use a combination of upper and lower case alphabets, numbers, and non-alphanumeric characters. It should never contain personal information. Change your passwords every 60 to 90 days.
- Disable all unnecessary programs and services to reduce potential vulnerabilities.
- Educate your end users to:
  - Read the End User License Agreement (EULA) and included documentation of applications they download and install on their computers.
  - Click **No** to any message asking for authorization to download and install software (unless the end users are certain that they can trust both the creator of the software they are downloading and the Web site source from where they are downloading the software).
  - Disregard unsolicited commercial email messages (spam), especially if the spam asks users to click a button or hyperlink.
- Configure Web browser settings that ensure a strict level of security.

  Trend Micro recommends requiring Web browsers to prompt users before installing ActiveX controls. To increase the security level for Internet Explorer (IE), go to **Tools** > **Internet Options** > **Security** and move the slider to a higher level. If this setting causes problems with Web sites you want to visit, click **Sites...**, and add the sites you want to visit to the trusted sites list.
- If using Microsoft Outlook, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages.
- Prohibit the use of peer-to-peer file-sharing services.
- Periodically examine the installed software on the computers on your network. If you find an application or file that WFBS-SVC cannot detect as an Internet threat, send it to Trend Micro:

  `http://subwiz.trendmicro.com/SubWiz`

  TrendLabs will analyze the files and applications you submit.

  Or end a message to the following address: `virusresponse@trendmicro.com`

For more information about best practices for computer security, visit the Trend Micro Web site and read the *Safe Computing Guide* and other security information.

http://www.trendmicro.com/en/security/general/virus/overview.htm

Appendix D

Troubleshooting and Frequently Asked Questions

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

The topics discussed in this appendix include:

- *Troubleshooting* on page D-2
- *Frequently Asked Questions (FAQs)* on page D-3
- *Product Exclusion List* on page D-4
- *Known Issues* on page D-7

Troubleshooting

This section helps you troubleshoot issues that may arise while sing WFBS-SVC

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.

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:

- Make sure the client computer can access the Internet.
- Logon to the WFBS-SVC console and verify that **Live Status > License Status > License** is enough.
- If you have limited bandwidth, check if it causes a connection timeout between the client and the Internet.
- If all else fails, contact Trend Micro support.

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.

Frequently Asked Questions (FAQs)

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

Where Can I Find My Registration Information?

Your activation code is available on the WFBS-SVC console under **Administration > License**.

The Activation Codes has 37 characters and looks like the following:

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

The Registration Key has 22 characters and looks like the following:

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

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

- Updates to the WFBS-SVC 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

When the full version expires, security updates will be disabled; when the trial 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-SVC. 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

You can also contact your reseller or Trend Micro Support.

Installation, Upgrade, and Compatibility

Which Agent installation method is best for my network environment?

See *Agent Installation Overview* on page 3-2 for a summary and brief comparison of the various Agent installation methods available.

Does WFBS-SVC 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.

How Can I Recover a Lost or Forgotten Password?

Access to the WFBS-SVC Security console requires a password which is first defined during registration and can be subsequently changed at any time. If you lost your password, you ca:

1. Check the email you received when you first signed up for WFBS-SVC.
2. Click the **Forgot your password?** link on the WFBS-SVC logon page.

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.

Do I Have the Latest Pattern File or Service Pack?

To find out if you have the latest pattern files:

1. From the Web console, click **Computers >** {group}. Check the **Virus Pattern** column on the right panel.

   OR

   From the Web console, click **Live status > System Status > Update > More info...**
2. Compare this to the latest pattern files at:

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

Product Exclusion List

This product exclusion list contains all of the Trend Micro products that are, by default, excluded from scanning.

TABLE D-1. Trend Micro Product Exclusion List

PRODUCT NAME	INSTALLATION PATH LOCATION
InterScan eManager 3.5x	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion ProgramDirectory=
ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion ProgramDirectory=
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=
InterScan Web Security Suite (IWSS)	HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite Program Directory= C:\Program Files\Trend Mircro\IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion ProgramDirectory=

TABLE D-1. Trend Micro Product Exclusion List (Continued)

PRODUCT NAME	INSTALLATION PATH LOCATION
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion ProgramDirectory={Installation Drive}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion ProgramDirectory=
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security\Current-Version HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

TABLE D-1. Trend Micro Product Exclusion List (Continued)

PRODUCT NAME	INSTALLATION PATH LOCATION
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\ Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\ Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= Get exclusion.txt file path from: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir Go to HomeDir path (for example, C:\Program Files\Trend Micro\Messaging Security Agent\) Open exclusion.txt C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

Known Issues

Known issues are features in WFBS-SVC software that may temporarily require a workaround. Known issues are documented in the Known Issues list available from the **Help** menu and the Trend Micro Update Center:

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

Trend Micro recommends that you always check the Known Issues list for information that could affect installation or performance.

Appendix E

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* on page E-2
- *Knowledge Base* on page E-2
- *Trend Community* on page E-2
- *Technical Support* on page E-3
- *Contacting Trend Micro* on page E-3
- *Sending Suspicious Files to Trend Micro* on page E-4
- *Trend Micro Virus Information Center* on page E-4
- *About TrendLabs* on page E-5

Product Documentation

The documentation for WFBS-SVC consists of the following:

- Online Help and User's Guide

  The WFBS-SVC *Online Help* and *User's Guide* are nearly identical. They describe 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.

  The *User's Guide* can be downloaded from the Trend Micro Update Center:

  http://www.trendmicro.com/download

- Agent Readme file

  The *Agent 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://go.trendmicro.com/smallbusinesssupport

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 a trial version of a product. Visit:

http://go.trendmicro.com/smallbusinesssupport

Trend Community

Get help, share your experiences, ask questions, and discuss security concerns in the forums with fellow users, enthusiasts, and security experts.

http://community.trendmicro.com/

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 E-3) 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:

Run the Case Diagnostic Tool. For more information, refer to*Using the Case Diagnostic Tool* on page E-3.

- Visit the following URL:

  http://go.trendmicro.com/smallbusinesscontact

  Follow the instructions for contacting support.
- 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://esupport.trendmicro.com/support/srf/questionentry.do

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 trial. 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.

Trend Micro 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

About 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 F

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-SVC 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 desktops, portable computers, and servers where 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.
Conventional Scan	A local scan engine on the client scans the client computer.
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.

Term	Description
False Positive	A false positive occurs when a Web site, URL or "infected" file is incorrectly determined by filtering software to be of an unwanted type. For example, a legitimate email between colleagues may be detected as spam if a job-seeking filter does not distinguish between resume (to start again) and résumé (a summary of work experience).
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.
Malware	A malware is a program that performs unexpected or unauthorized actions. It is a general term used to refer to viruses, Trojans, and worms. Malware, depending on their type, may or may not include replicating and non-replicating malicious code.
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	A server that helps scan clients so clients do not have to complete the whole scanning process themselves.
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.
True File Type	Files can be renamed to disguise their actual type. When set to IntelliScan, the Client/Server Security Agent will confirm a file's true type by opening the file header and checking its internally registered data type.
Update	Agents that act as update sources for other Agents.
Virus Pattern	The Trend Micro Scan Engine uses a data file called the virus pattern file. The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching, to identify viruses and other Internet threats. New virus pattern files are created and released several times a week, and any time a particularly threat is discovered.
Web console	The Web console is a centralized Web-based management console. You use it to configure the settings of Client/Server Security Agents which protect all your remote desktops and servers.
WFBS-SVC Server	The WFBS-SVC Server communicates with Client/Server Security Agents installed on clients. The WFBS-SVC Server also hosts the Web console, the centralized Web-based management console for the entire WFBS-SVC solution. It is hosted at Trend data centers.

Index