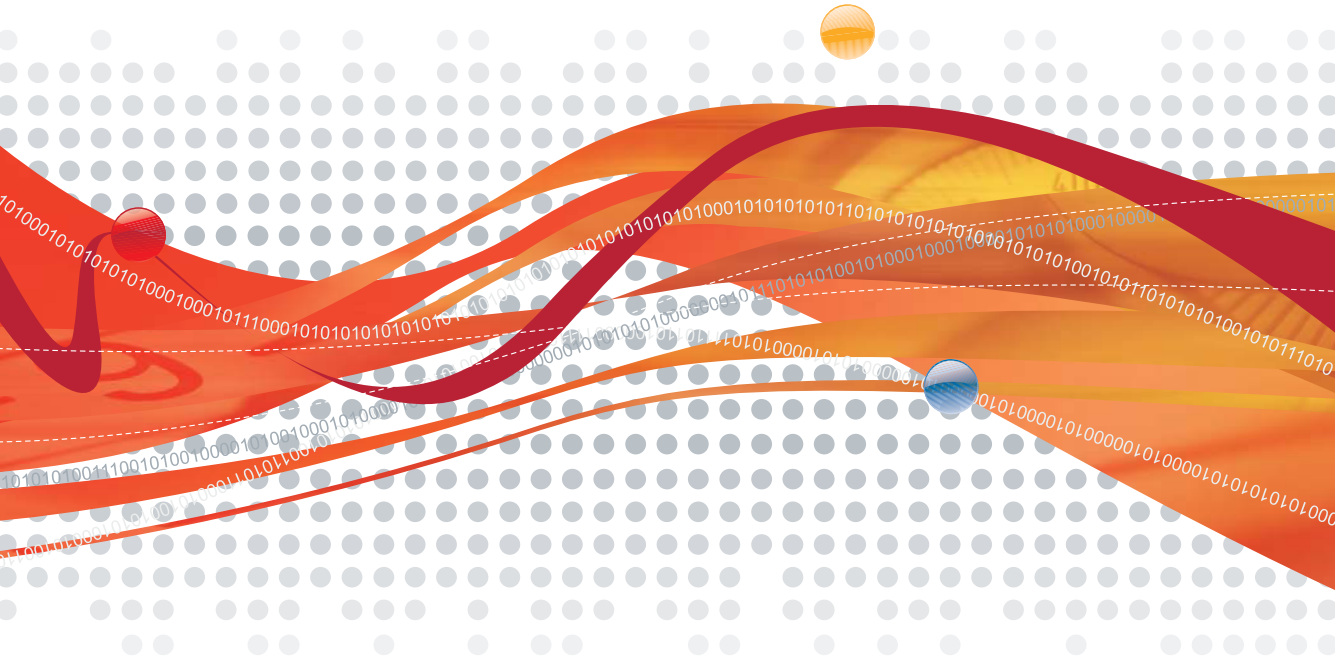
TREND MICRO

# Worry-Free™ Business Security Advanced5

for Small and Medium Business



## Getting Started 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 Getting Started Guide, which are available from Trend Micro's Web site at:

**http://www.trendmicro.com/download/default.asp**

NOTE: A license to the Trend Micro Software includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Thereafter, you must renew Maintenance on an annual basis by paying Trend Micro's then-current Maintenance fees to have the right to continue receiving product updates, pattern updates, and basic technical support.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

**http://www.trendmicro.com/en/purchase/license/overview.htm**



Document Part No.: WAEM53521

Release Date: May 2008

The Trend Micro™ Worry-Free™ Business Security Advanced Getting Started Guide is intended to introduce the main features of the software and installation instructions for your production environment. You should read 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 online Knowledge Base at Trend Micro's Web site.

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

**`www.trendmicro.com/download/documentation/rating.asp`**

# Contents

## Preface



## Chapter 1: Introducing Trend Micro Worry-Free Business Security Advanced

# Preface

Welcome to the Trend Micro™ Worry-Free™ Business Security Advanced 5.0 Getting Started Guide. This book contains information about deploying, installing or upgrading the product, getting started with the product, and general information about threats.

This preface discusses the following topics:

# Audience

Worry-Free Business Security Advanced (WFBS-A) Administrators for small- to medium-sized businesses who intend to install or upgrade to Trend Micro™ Worry-Free™ Business Security Advanced 5.0.

# Product Documentation

The Worry-Free Business Security Advanced bundle consists of two components—a hosted/offsite email protection service (InterScan Messaging Hosted Security) and on-premise server, desktop, and email protection software. The documents for InterScan Messaging Hosted Security are available at the following location:

**http://us.trendmicro.com/us/products/enterprise/interscan-messaging-hosted-security/**

The documentation for Worry-Free Business Security Advanced consists of the following:

- Online Help
  Web-based documentation accessible from the Web console.

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

  *Who should use the online help?*

  WFBS-A Administrators who need help with a particular screen.

- Getting Started Guide
  The *Getting Started Guide* provides instructions to install/upgrade the product and get started. It provides a description of the basic features and default settings of Worry-Free Business Security Advanced.

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

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

  *Who should read this guide?*

WFBS-A Administrators who want to install and get started with Worry-Free Business Security Advanced.

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

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

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

  *Who should read this guide?*

  WFBS-A Administrators who need to customize, maintain, or use Worry-Free Business Security Advanced.

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

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

  **http://esupport.trendmicro.com**

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

**www.trendmicro.com/download/documentation/rating.asp**

---

**Note:** This guide assumes that you are using the Worry-Free Business Security Advanced version of the product. If you are using the Worry-Free Business Security version, the information in this guide is applicable, but you will not be able to use the features that belong to Messaging Security Agent. See *Worry-Free Business Security and Worry-Free Business Security Advanced* on page 4-5.

---

## What Information Can I Find in the Getting Started Guide?

**Chapter 1**: A brief introduction to the key features of Worry-Free Business Security Advanced, security risks, and how Worry-Free Business Security Advanced can combat these threats. See *Introducing Trend Micro Worry-Free Business Security Advanced* on page 1-1.

**Chapter 2**: Overview of the entire installation process. See *Getting Started with Worry-Free Business Security Advanced* on page 2-1.

**Chapter 3**: Information on pilot deployment and its benefits. See *Deployment Planning* on page 3-1.

**Chapter 4**: Instructions to install Worry-Free Business Security Advanced and verify the installation. See *Installing Worry-Free Business Security Advanced* on page 4-1.

**Chapter 5**: Instructions to upgrade or migrate to Worry-Free Business Security Advanced. See *Upgrading/Migrating Worry-Free Business Security Advanced Security* on page 5-1.

**Chapter 6**: A brief description of the Web console. See *Web Console Overview* on page 6-1.

**Chapter 7**: High-level instructions on how to configure and manage security tasks using Worry-Free Business Security Advanced. See *Configuring Security Settings* on page 7-1.

**Chapter 8**: Instructions on finding support. See *Technical Support* on page 8-1.

**Appendix A**: Tips to get the most out of Worry-Free Business Security Advanced. See *Best Practices to Protect Your Computers and Network* on page A-1.

# Document Conventions and Terms

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

**TABLE P-1. Descriptions of conventions and terms**

| 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 |
| Security Server | The Security Server hosts the Web console, the centralized Web-based management console for the entire Worry-Free Business Security Advanced solution. |
| Web console | The Web console is a centralized Web-based management console that manages all the Agents. The Web console resides on the Security Server. |
| Agent/CSA | The Client/Server Security Agent or Messaging Security Agent. Agents protect the Client it is installed on. |
| Client | Clients are Exchange servers, desktops, portable computers, and servers where a Messaging Security Agent or a Client/Server Security Agent is installed. |

Chapter 1

# Introducing Trend Micro Worry-Free Business Security Advanced

This chapter includes the following topics:

# Overview of Worry-Free Business Security Advanced

Trend Micro™ Worry-Free™ Business Security Advanced (WFBS-A) protects your business and its reputation against data theft, risky Web sites, and overwhelming spam. Our safer, smarter, simpler security blocks Web-based threats and other malware to protect your business assets and customer information.

Only Trend Micro offers Web threat protection that addresses the exponential growth of Web threats with constant updates that will not slow your PCs down. Our knowledge base rapidly deploys to defend all our customers like a global neighborhood watch.

Worry-Free Business Security Advanced includes InterScan™ Messaging Hosted Security to block spam before it reaches your network. Worry-Free Business Security Advanced protects Microsoft™ Exchange and Small Business Servers, Microsoft Windows™ servers, PCs, and portable computers.

# What's New in This Release?

This version of Worry-Free Business Security Advanced for Small and Medium Business (SMB) brings a host of benefits to small and medium businesses that lack dedicated resources for antivirus management. This version of Worry-Free Business Security Advanced inherits all the features of previous versions and provides the following new features:

## New Security Server Features

- **Location Awareness.** Worry-Free Business Security Advanced can identify the location of a Client based on Server Gateway information. Administrators can have different security settings based on the location of the Client (roaming or within in the office).
- **Threat Status.** View Web Reputation and Behavior Monitoring statistics on the Live Status screen.
- **Plug-in Manager.** Plug-in programs are designed to add new features and security capabilities into Worry-Free Business Security Advanced, and enhance the

product's features. Plug-in Manager facilitates the installation, deployment and management of plug-in programs.

- **User Interface.** Security Server now comes with a new and improved user interface.

## New Client/Server Security Agent Features

- **Windows Vista Support.** Client/Server Security Agents can now be installed on Windows Vista (32-bit and 64-bit) computers. Refer to Worry-Free Business Security Advanced *Administrator's Guide Appendix D* for a comparison of the CSA features on different platforms.
- **Behavior Monitoring.** Behavior Monitoring protects Clients from unauthorized changes to the operating system and other programs.
- **Web Reputation Services.** Web Reputation Services evaluates the potential security risk of each requested URL by querying the Trend Micro Security database at the time of each HTTP request.
- **Instant Message Content Filtering.** Instant Message Content Filtering can restrict the use of certain words or phrases while using instant messaging applications.
- **Software Protection.** With Software Protection, Worry-Free Business Security Advanced can protect .exe and .dll files in particular folders on Clients.
- **POP3 Mail Scan.** POP3 Mail Scan protects Clients against security risks transmitted through email messages. POP3 Mail Scan can also detect spam.

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

- **TrendSecure™.** TrendSecure comprises a set of browser-based tools (TrendProtect and Transaction Protector) that enable users to surf the Web securely. TrendProtect warns users about malicious and Phishing Web sites. Transaction Protector determines the safety of your wireless connection by checking the authenticity of the access point and includes a tool to encrypt personal information users type into Web pages.
- **Plug-in Manager Support.** Manage additional plug-ins for Client/Server Security Agent from the Security Server.

- **Language Packs.** Client/Server Security Agents can now display the interface based on the locale language.
- **User Interface.** Client/Server Security Agent now comes with a new and improved user interface.

### New Messaging Security Agent Features

**Email Reputation**. Enable Trend Micro Email Reputation Service to block messages from known and suspected spam sources.

## What's Included in Worry-Free Business Security Advanced

- The Web console manages all Clients from a single location.
- Trend Micro Security Server, which hosts the Web console, downloads updates from the Trend Micro ActiveUpdate Server, collects and stores logs, and helps control virus outbreaks.
- Trend Micro Client/Server Security Agent, which protects Windows Vista/2000/XP/Server 2003/Server 2008 computers from viruses, spyware/grayware, Trojans, and other threats.
- Trend Micro Messaging Security Agent, which scans email messages for threats and spam.

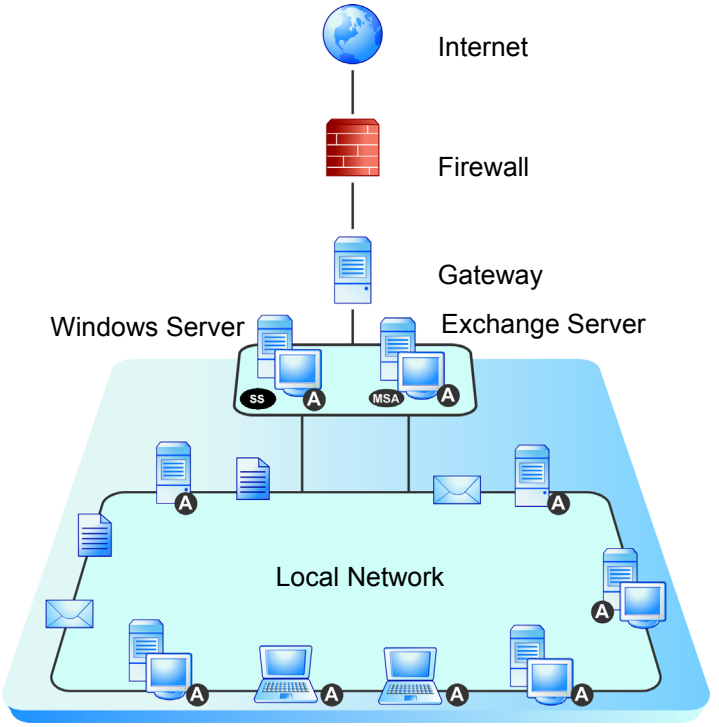



**FIGURE 1-1. Worry-Free Business Security Advanced protects desktops, servers, and Exchange servers**

| Symbol | Description |
|---|---|
| A | Client/Server Security Agent installed on Clients |
| MSA | Messaging Security Agent installed on an Exchange server |
| SS | Security Server installed on a Windows server |

## Web Console

The Web console is a centralized, Web-based, management console. Use the Web console to configure the settings of Client/Server Security Agents and Messaging Security Agents, which protect the Exchange servers, desktops, and servers on the

network. The Web console is installed when you install the Trend Micro Security Server and uses Internet technologies such as ActiveX, CGI, HTML, and HTTP/HTTPS.

Also use the Web console to:

- Deploy the Client/Server Security Agent program to desktops, notebooks, and servers.
- Deploy the Messaging Security Agent program to an Exchange server.
- Combine desktops and portable computers and servers into logical groups for simultaneous configuration and management.
- Set antivirus and anti-spyware scan configurations and start Manual Scan on a single group or on multiple groups.
- Receive notifications and view log reports for virus activities.
- When spyware or viruses are detected on Clients, receive notifications and send outbreak alerts through email messages, SNMP Trap, or Windows Event Log.
- Control outbreaks by configuring and enabling Outbreak Prevention.

## Security Server

At the center of Worry-Free Business Security Advanced is the Security Server (indicated by **SS** in Figure 1-1). The Security Server hosts the Web console, the centralized Web-based management console for the entire Worry-Free Business Security Advanced solution. The Security Server installs Security Agents to the computers on your network and along with the Security Agents, form a client-server relationship. The Security Server enables viewing security status information, viewing Clients, configuring system security, and downloading components from a centralized location. The Security Server also contains the database where it stores logs of detected Internet threats being reported to it by the Security Agents.

The Trend Micro Security Server performs these important functions:

- Installs, monitors, and manages Agents on the network
- Downloads virus pattern files, spyware pattern files, scan engines, and program updates from the Trend Micro update server, and then distributes them to Agents

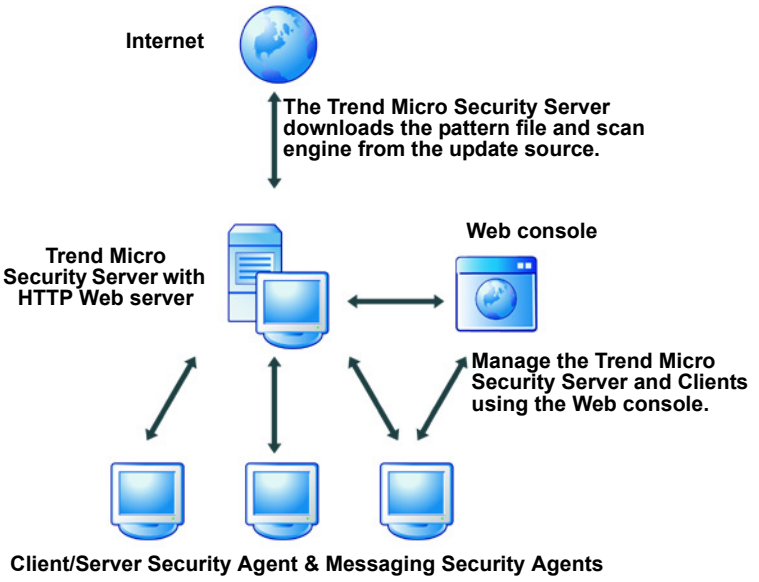



**FIGURE 1-2. How Client/Server communication through HTTP works**

## Client/Server Security Agent

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

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

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

## Messaging Security Agent

Protect Exchange servers from viruses by installing the Messaging Security Agent (indicated by **MSA** in Figure 1-1) on each Exchange server. The Messaging Security Agent protects the Exchange server against viruses, Trojans, worms, and other malware. It also provides spam blocking, content filtering, and attachment blocking for added security. The Messaging Security Agent provides three methods of scanning–Real-time Scan, Scheduled Scan, and Manual Scan.

The Messaging Security Agent reports to the Trend Micro Security Server from which it was installed. The Messaging Security Agent sends events and status information to the Security Server in real time. View the events and status information from the Web console.

## Scan Engine

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

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

Rather than scan every byte of every file, the engine and pattern file work together to identify not only tell-tale characteristics of the virus code, but the precise location within a file where a virus would hide. If Worry-Free Business Security Advanced detects a virus, it can remove it and restore the integrity of the file.

The scan engine removes old virus patterns (to save disk space) and incrementally updates pattern files (to reduce bandwidth).

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. Worry-Free Business Security Advanced 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 that the scan engine cannot handle
- 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**

## Virus Pattern File

The Trend Micro scan engine uses an external data file, called the virus pattern file. It contains information that helps Worry-Free Business Security Advanced identify the latest viruses and other Internet threats such as Trojan horses, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly threat is discovered.

All Trend Micro antivirus programs using the ActiveUpdate function can detect the availability of a new virus pattern file on the Trend Micro server. Administrators can

schedule the antivirus program to poll the server every week, day, or hour to get the latest file.

**Tip:** Trend Micro recommends scheduling automatic updates at least hourly. The default setting for all Trend Micro products is hourly.

Download virus pattern files from the following Web site (information about the current version, release date, and a list of all the new virus definitions included in the file is available):

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

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching.

## Virus Cleanup Engine

Damage Cleanup Services (DCS) makes use of a scanning and cleanup tool called the Virus Cleanup Engine (DCE) to find and repair damage caused by viruses and other Internet threats. The Virus Cleanup Engine can find and clean viruses, Trojans, and other malware. The DCE is essentially a software agent that makes use of a database to find targeted Clients and evaluate whether viruses or other Internet threats have affected them. DCE resides on a single machine and deploys to the targeted computers on the network at the time of scanning.

The Virus Cleanup Engine uses the Virus Cleanup Pattern to restore damage caused by the latest known viruses, malware, or other Internet threats. DCS regularly updates these templates. Trend Micro recommends to update the components immediately after installing and activating Worry-Free Business Security Advanced. TrendLabs updates the Virus Cleanup Pattern frequently.

## Common Firewall Driver

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

### Network Virus Pattern File

The Network Virus Pattern file contains a regularly updated database of packet-level network virus patterns. Trend Micro updates the network virus pattern file frequently, as often as hourly, to ensure Worry-Free Business Security Advanced can identify new network viruses.

### Vulnerability Pattern File

Worry-Free Business Security Advanced deploys the Vulnerability Pattern file after updating components. The Vulnerability Pattern file is used in the **Outbreak Defense > Potential Threat** screen when the Scan for Vulnerability Now tool is used, when scheduled Vulnerability Assessment is triggered, or whenever a new Vulnerability Pattern file is downloaded. Soon after downloading the new file, Agents starts scanning Clients for vulnerabilities.

## 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.

### Viruses/Malware

A computer virus is a program – a piece of executable code – that has the unique ability to replicate. Viruses 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 viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they 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 viruses, Trojans do not replicate but can be just as destructive.

An application that claims to rid your computer of viruses when it actually introduces viruses onto 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 viruses, 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.

Client/Server Security Agents and Messaging Security Agents can detect viruses during Antivirus scanning. The Trend Micro recommended action for viruses is *clean*.

## Spyware/Grayware

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

- **Spyware.** Spyware is computer software that is installed on a computer without the user's consent or knowledge and collects and transmits personal information.
- **Dialers.** Dialers are necessary to connect to the Internet for non-broadband connections. Malicious dialers are designed to connect through premium-rate numbers instead of directly connecting to your ISP. Providers of these malicious dialers pocket the additional money. Other uses of dialers include transmitting personal information and downloading malicious software.

- **Hacking Tools.** A hacking tool is a program, or a set of programs, designed to assist hacking.
- **Adware.** Adware, or advertising-supported software, is any software package, which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- **Keyloggers.** A keylogger is computer software that logs all the keystrokes of the user. This information could then be retrieved by a hacker and used for his/her personal use.
- **Bots.** A bot (short for "robot") is a program that operates as an agent for a user or another program or simulates a human activity. Bots, once executed, can replicate, compress, and distribute copies of themselves. Bots can be used to coordinate an automated attack on networked computers.

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

## Network Viruses

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

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

## Spam

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

## Intrusions

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

## Malicious Behavior

Malicious Behavior refers to unauthorized changes by a software to the operating system, 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 keystroke listener is an online version of a keylogger. See *Spyware/Grayware* on page 1-12 for more information.

## Packers

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

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

## Phishing Incidents

A Phishing incident starts with an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click a link that will redirect their browsers to a fraudulent Web site. Here the user is asked to update personal information such as passwords, social security numbers, and credit

card numbers in an attempt to trick a recipient into providing private information that may be used for identity theft.

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

### Mass-Mailing Attacks

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

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

## How Worry-Free Business Security Advanced Protects Your Computers and Network

The following table describes how the different components of Worry-Free Business Security Advanced protect your network from threats.

**TABLE 1-1. Threats and Worry-Free Business Security Advanced Protection**

| Threat | Worry-Free Business Security Advanced Protection |
|---|---|
| • **Virus/Malware.** Virus, Trojans, Worms, Backdoors, and Rootkits<br>• **Spyware/Grayware.** Spyware, Dialers, Hacking tools, Password cracking applications, Adware, Joke programs, and Keyloggers | Antivirus and Anti-spyware Scan Engines along with Pattern Files in Client/Server Security Agent and Messaging Security Agent |
| Virus/Malware and Spyware/Grayware transmitted through email messages and spam | POP3 Mail Scan in Client/Server Security Agent and IMAP Mail Scan in Messaging Security Agent |

**TABLE 1-1. Threats and Worry-Free Business Security Advanced Protection**

| Threat | Worry-Free Business Security Advanced Protection |
|---|---|
| Network Worms/Viruses | Firewall in Client/Server Security Agent |
| Intrusions | Firewall in Client/Server Security Agent |
| Conceivably harmful Web sites/Phishing sites | Web Reputation Services 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 |
| Online keystroke listeners | Transaction Protector in Client/Server Security Agent |
| Explicit/restricted content in IM applications | IM Content Filtering in Client/Server Security Agent |

Worry-Free Business Security Advanced is a multi-tier application that uses the following modules to protect your Exchange servers, desktops and servers:

## Antivirus

- **Scan Engine (Client/Server Security Agent and Messaging Security Agent).** The scan engine uses the virus pattern file to detect viruses 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 TrendLabs capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to patterns in the virus pattern file, searching for a match.

- **Virus Pattern.** A file that helps the Security Agents identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.
- **Virus Cleanup Pattern.** Used by the virus cleanup engine, this template helps identify Trojan files and Trojan processes, worms, and spyware so the engine can eliminate them.

- **Virus Cleanup Engine.** The engine that Cleanup Services uses to scan for and remove Trojan files and Trojan processes, worms, and spyware.

## Anti-spyware

- **Spyware Scan Engine (32-bit).** A separate scan engine that scans for, detects, and removes spyware from infected computers and servers running on i386 (32-bit) operating systems (Windows Vista, Windows XP, Windows Server 2003, and Windows 2000).
- **Spyware Scan Engine (64-bit).** Similar to the spyware scan engine for 32-bit systems, this scan engine scans for, detects, and removes spyware on x64 (64-bit) operating systems (Windows Vista x64, Windows XP Professional x64 Edition, Windows 2003 x64 Edition).
- **Spyware Pattern.** Contains known spyware signatures and is used by the spyware scan engines (both 32-bit and 64-bit) to detect spyware 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 real-time anti-spyware scanning.

## Anti-spam

- **Spam engine.** Detects unsolicited commercial email messages (UCEs) or unsolicited bulk email messages (UBEs), otherwise known as spam.
- **Spam pattern.** Contains spam definitions to enable the spam engine to detect spam in POP3 and IMAP email messages.
- **Email Reputation Services (ERS).** Stops up to 80 percent of spam before it hits the gateway and floods the messaging infrastructure.

## Firewall

- **Common Firewall Engine 32-bit.** The Firewall uses this engine, together with the network virus pattern file, to protect computers running Windows Vista/2000/XP/Server 2003 from hacker attacks and network viruses.
- **Common Firewall Pattern.** Like the virus pattern file, this file helps Worry-Free Business Security Advanced identify network viruses.

## Web Reputation

**Trend Micro Security database.** Web Reputation evaluates the potential security risk of the requested Web page before displaying it. Depending on rating returned by the database and the security level configured, Client/Server Security Agent will either block or approve the request

## TrendProtect

**Trend Micro Security database.** TrendProtect evaluates the potential security risk of the hyperlinks displayed on a Web page. Depending on 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.** The Software Protection List comprises programs that can modify the contents of files or folders. If a program is not in the list, it cannot create, modify, or delete files or folders.

## Behavior Monitoring

- **Behavior Monitor Core Drivers (32-bit).** This driver detects process behavior on Clients.
- **Behavior Monitor Core Service (32-bit).** CSA uses this services to handle the Behavior Monitor Core Drivers.
- **Policy Enforcement Pattern.** The list of policies configured on the Security Server that must be enforced by Agents.
- **White Listing Pattern.** List of Trend Micro-accepted companies whose software is safe to use.
- **Behavior Monitor Configuration Pattern.** This pattern stores the default Behavior Monitoring Policies.

### Transaction Protector

- **Wi-Fi Advisor.** Checks the safety of wireless networks.
- **Password ClipBoard.** An on-screen keyboard for securely entering user names and passwords that hides typed text from keyloggers.

### Content Filtering

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

### 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 to the scan engine to scan for known vulnerabilities.

### Live Status and Notifications

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

## Other Supplementary Trend Micro Products

Worry-Free Business Security Advanced offers comprehensive protection for Exchange servers, Windows desktops and servers on a local network; however, it does not provide a solution for gateway devices and non-Windows operating systems.

To expand your protection, consider combining Worry-Free Business Security Advanced with Trend Micro™ InterScan VirusWall for Small and Medium Business.

- InterScan VirusWall is the most comprehensive gateway security software protecting businesses from viruses, spyware, spam, phishing, bots, and inappropriate content, before they can harm your network.

Chapter 2

# Getting Started with Worry-Free Business Security Advanced

This chapter outlines the different phases involved in installing and deploying Worry-Free Business Security Advanced within your organization. This chapter includes the following topics:

# Phase 1: Deployment Planning

Planning the Worry-Free Business Security Advanced deployment includes the following tasks:

1. Deploying a Pilot Installation. Refer to *Pilot Deployment* on page 3-2 for more information.
2. Verifying system requirements. Refer to *System Requirements* on page 4-2 for more information.
   - for servers
   - for desktop and portable computers
   - for Exchange servers
3. Determining where to install the Security Server. Refer to *Determining Where to Install the Security Server* on page 3-3 for more information.
4. Identifying the number of clients. Refer to *Identifying the Number of Clients* on page 3-3 for more information.
5. Planning for network traffic. Refer to *Planning for Network Traffic* on page 3-4 for more information.
6. Determining desktop and server groups. Refer to *Determining the Number of Desktop and Server Groups* on page 3-7 for more information.
7. Choosing installation/deployment options for Client/Server Security Agents. Refer to *Choosing Deployment Options for Agents* on page 3-8 for more information.

# Phase 2: Installing Security Server

This phase includes the following tasks:

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

**Tip:** Update the System Checklists section of the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide*. Reference this information while installing Worry-Free Business Security Advanced.

- Installing or upgrading Worry-Free Business Security Advanced. Refer to *Worry-Free Business Security Advanced Installation Methods* on page 4-11 or *Upgrading/Migrating Worry-Free Business Security Advanced Security* on page 5-1 for more information.
- Verifying the installation. Refer to *Verifying the Installation* on page 4-41 for more information.

## Phase 3: Installing Agents

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

**Note:** Refer to *Choosing Deployment Options for Agents* on page 3-8 for an overview of installing Agents and to the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide* for detailed instructions.

- Selecting an installation method
- Installing or upgrading Agents
- Verifying the installation
- Testing the installation

## Phase 4: Configuring Security Options

**Note:** Refer to *Configuring Security Settings* on page 7-1 for an overview of the configuration options and to the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide* for detailed instructions.

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

- Configuring desktop and server groups
- Configuring Exchange servers
- Configuring preferences

Chapter 3

# Deployment Planning

The steps in this phase help you develop a plan for Worry-Free Business Security Advanced 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.

This chapter includes the following topics:

# Pilot Deployment

Before performing a full-scale deployment, Trend Micro recommends that you first conduct a pilot deployment in a controlled environment. A pilot deployment provides an opportunity to determine how features work and what level of support you will likely need after full deployment.

It also gives your installation team a chance to rehearse and refine the deployment process and test if your deployment plan meets your organization's antivirus needs.

**Tip:** Although this phase is optional, Trend Micro recommends conducting a pilot deployment before doing a full-scale deployment.

## Choosing a Pilot Site

Choose a pilot site that matches your production environment. Try to simulate the type of network topology that would serve as an adequate representation of your production environment.

## Creating a Rollback Plan

Trend Micro recommends creating a disaster recovery or rollback plan in case there are issues with the installation or upgrade process.

This process should take into account company information security policies, as well as technical specifics.

## Deploying Your Pilot

Evaluate the different installation methods (Typical Installation, Custom Installation, Silent Installation) to see which one is suitable for your environment.

### Evaluating Your Pilot Deployment

Create a list of successes and failures encountered throughout the pilot process. Identify potential pitfalls and plan accordingly for a successful deployment. This pilot evaluation plan can be rolled into the overall production deployment plan.

## Determining Where to Install the Security Server

Worry-Free Business Security Advanced is flexible enough to accommodate a variety of network environments. For example, you can position a firewall between the Trend Micro Security Server and Clients running the Client/Server Security Agent, or position both the Trend Micro Security Server and all Clients behind a single network firewall.

If managing more than one site, having a security server at the main site as well as at each managed site will reduce bandwidth usage between the main site and managed sites, and speed up pattern deployment rates.

If Clients have the Windows XP Firewall enabled, Worry-Free Business Security Advanced will automatically add it to the Exception list.

---

**Note:** If a firewall is located between the Trend Micro Security Server and its Clients, you must configure the firewall to allow traffic between the Client listening port and Trend Micro Security Server's listening port.

---

## Identifying the Number of Clients

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

If your network has different Windows operating systems, such as Windows 2000, XP, Server 2003 or Vista, identify how many Clients are using a specific Windows version. Use this information to decide which Client deployment method will work best in your environment.Refer to *Choosing Deployment Options for Agents* on page 3-8.

**Note:** A single Security Server installation can manage up to 2500 Clients. If you have more Clients than this, Trend Micro suggests installing more than one Security Server.

# Planning for Network Traffic

When planning for deployment, consider the network traffic that Worry-Free Business Security Advanced will generate. Worry-Free Business Security Advanced generates network traffic when the Security Server and Clients communicate with each other.

The Security 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

Clients generate traffic when:

- Starting up
- Shutting down
- Generating logs
- Switching between roaming mode and normal mode
- Performing scheduled updates
- Performing manual updates (“Update Now”)

**Note:** Other than updates, all the other actions generate insignificant traffic.

## Network Traffic During Pattern File Updates

Significant network traffic is generated whenever TrendLabs releases an updated version of any of the following items:

**TABLE 3-1. Updatable Components**

| Component | Sub-component |
|---|---|
| Antivirus | • Virus Pattern<br>• Virus Scan Engine 32-bit<br>• Virus Scan Engine 64-bit<br>• Virus Cleanup Template<br>• Virus Cleanup Engine 32-bit<br>• Virus Cleanup Engine 64-bit<br>• Messaging Security Agent scan Engine 32-bit<br>• Messaging Security Agent scan Engine 64-bit<br>• IntelliTrap Exception Pattern<br>• IntelliTrap Pattern |
| Anti-spyware | • Spyware Scan Engine 32-bit<br>• Spyware scan Engine 64-bit<br>• Spyware Pattern<br>• Spyware Active-monitoring Pattern |
| Anti-spam | • Anti-spam Pattern<br>• Anti-spam Engine 32 -bit<br>• Anti-spam Engine 64-bit |
| Outbreak Defense | • Vulnerability Pattern |
| Network Virus | • Common Firewall Pattern<br>• Common Firewall Engine 32-bit<br>• Common Firewall Engine 64-bit<br>• TDI Driver 32-bit<br>• TDI Driver 64-bit<br>• WFP Driver 32-bit<br>• WFP Driver 64-bit |
| Web Reputation | • Web Reputation Engine 32-bit<br>• Web Reputation Engine 64-bit |
| Behavior Monitoring | • Behavior Monitor Core Drivers 32-bit<br>• Behavior Monitor Core Service 32-bit<br>• Policy Enforcement Pattern<br>• White Listing Pattern<br>• Behavior Monitor Configuration Pattern |

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

Regularly updated Clients only have to download the incremental pattern, which is approximately 5KB to 200KB. The full pattern is approximately 20MB when compressed and takes substantially longer to download.

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

### Using Update Agents to Reduce Network Bandwidth

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

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

## Deciding on a Dedicated Server

When selecting a server that will host Worry-Free Business Security Advanced, consider the following:

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

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

# Location of the Program Files

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

The default Client installation path is:

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

# Determining the Number of Desktop and Server Groups

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

---

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

---

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

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

# Choosing Deployment Options for Agents

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

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

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

---

**Note:** Remote install works only with Windows Vista/2000/XP (Professional Edition only) and Server 2003.

---

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

Worry-Free Business Security Advanced includes a tool called the Vulnerability Scanner, which can help you detect computers that are not protected by Worry-Free Business Security Advanced. Once Vulnerability Scanner detects an unprotected computer, it deploys Client/Server Security Agent to it. When you enter a range of IP addresses, the Vulnerability Scanner checks every computer within the specified range and reports the current antivirus software version (including third-party software) installed on each computer.

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

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

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

For more information about the installation methods, refer to the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide*.

Chapter 4

# Installing Worry-Free Business Security Advanced

This section provides information you will need to understand to install Worry-Free Business Security Advanced. The topics discussed in this chapter include:

# System Requirements

To install Worry-Free Business Security Advanced, the following are required:

**TABLE 4-1. Installation Requirements**

| Worry-Free Business Security Advanced Component | Minimum System Requirement | | | Other Requirements |
|---|---|---|---|---|
| | CPU/RAM | Disk Space | Operating System | |
| Security Server | For X86: Intel™ Pentium™ or compatible processor: 512MB<br>For X64: Supports AMD™ 64 technology and Intel™ EM64T technology: 1GB | 1.2GB | Microsoft™ Windows Vista (or SP1)<br>Windows Home Server<br>Windows Server 2008/Server 2003 (R2) (SP1 or later)<br>Windows XP (SP2 or later)<br>Windows 2000 (SP4)<br>SBS 2000/SBS 2003(R2) | Web Server:<br>Windows 2000/SBS 2000: IIS 5.0<br>Windows Server 2003/Homeserver/SBS 2003(R2): IIS 6.0<br>Windows Server 2008: IIS 7.0<br>Apache Web server 2.0.54 or later, except 2.0.56-2.0.59, 2.2.2, and 2.2.3 (for Windows 2000 SP4/XP SP2 or later/ Server 2003 (R2) (SP1 or later) only) |
| Web Console | NA | NA | NA | Internet Explorer™ 6.0 or later (32bit only, 64bit not supported)<br>Reports (.pdf) require Acrobat Reader™ version 4.x or above<br>Display: Monitor that supports 1024 x 768 resolutions at high colors |

| | | | | |
|---|---|---|---|---|
| Client/Server<br><br>Security Agent | For X86: Intel Pentium or compatible processor: Windows 2000/SBS 2000/XP/Server 2003/Homeserver/SBS 2003: 256MB, (recommended 512MB)<br><br>For X64: Supports AMD 64 technology and Intel EM64T technology: Windows Vista™/Server 2008/XP(x64)/ Server 2003 (X64): 512MB<br><br>Windows Vista/Server 2008 for X64: 1GB | 300MB/ 500MB for Update Agents | Windows Home Server<br><br>Windows Server 2008/Server 2003 (R2) (SP1 or later)<br><br>Windows XP (SP2 or later)<br><br>Windows 2000 (SP4)<br><br>SBS 2000/SBS 2003(R2) | Internet Explorer 5.5 SP2 or later required to perform Web setup<br><br>Display: Monitor that supports 800 x 600 resolution at 256 colors or higher<br><br>Terminal Service: Citrix Presentation Server™ and Remote Desktop |
| Messaging Security Agent | 1GB | 1GB | Windows 2000 SP4<br><br>Windows Server 2003 (R2) SP1 or later<br><br>SBS 2000/SBS 2003 SP1 (R2) | Mail Server: Exchange 2000 SP3/Exchange 2003 SP1/ Exchange 2007<br><br>Web Server:<br><br>Windows 2000/SBS 2000: IIS 5.0<br><br>Windows Server 2003/SBS 2003(R2): IIS 6.0<br><br>Apache Web server 2.0.54 or later<br><br>Exchange Intelligent Message Filter (only for SBS 2003 SP1) |

**Note:** CSA supports Gigabit Network Interface Card (NIC) and Tablet PCs.

## Other Requirements

- Administrator or Domain Administrator access on the computer hosting the Security Server
- File and printer sharing for Microsoft Networks installed
- Transmission Control Protocol/Internet Protocol (TCP/IP) support installed

**Note:** If Microsoft ISA Server or a proxy product is installed on the network, you need to enable the HTTP port (80 or 8080) and SSL port (443 or 4343) to enable access to the Web console and to ensure that client-server communication can be established.

# Choosing Your Edition

## Full Version and Evaluation Version

You can install either a full version of Worry-Free Business Security Advanced or a free, evaluation version.

- **Full version.** Comes with technical support, virus pattern downloads, real-time scanning, and program updates for one year. You can renew a full version by purchasing a maintenance renewal. You need an Activation Code to install the full version.
- **Evaluation version.** Provides real-time scanning and updates for 30 days. You can upgrade from a evaluation version to a full version at any time. You do not need an Activation Code to install the evaluation version.

## Registration Key and Activation Codes

Your version of Worry-Free Business Security Advanced comes with a Registration Key. During installation, Worry-Free Business Security Advanced prompts you to enter an Activation Code.

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

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

If you do not have either the Registration Key or Activation Code, you can still install the evaluation version. The evaluation version has all the same functionality as the full version, and if you upgrade within 30 days, all of your settings will automatically be upgraded to the full version. To find out more information contact your Trend Micro sales representative (see *Contacting Trend Micro* on page 8-2).

---

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

---

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

The Activation Code that you receive from Trend Micro depends on the product purchased.

The following table lists the features supported for each edition.

**TABLE 4-2. Features Available by Product Editions**

| Features | Worry-Free Business Security | Worry-Free Business Security Advanced |
|---|---|---|
| Component Updates | Yes | Yes |
| Antivirus/Anti-spyware | Yes | Yes |
| Firewall | Yes | Yes |
| Web Reputation | Yes | Yes |
| Behavior Monitoring | Yes | Yes |
| TrendSecure | Yes | Yes |
| Instant Messaging Content Filtering | Yes | Yes |
| Mail Scan (POP3) | Yes | Yes |
| Anti-Spam (POP3) | Yes | Yes |
| Mail Scan (IMAP) | No | Yes |

**TABLE 4-2. Features Available by Product Editions**

| Features | Worry-Free Business Security | Worry-Free Business Security Advanced |
|---|---|---|
| Anti-Spam (IMAP) | No | Yes |
| Email Message Content Filtering | No | Yes |
| Attachment Blocking | No | Yes |

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

**TABLE 4-3. License Status Consequences**

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

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

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

## Other Antivirus Applications

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

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

## Known Compatibility Issues

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

### Databases

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

### Other Firewall Applications

Trend Micro recommends removing 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 Firewall. However, if you want to run ICF or any other third-party firewall, add the Trend Micro Security Server listening ports to the firewall exception list (see *Understanding Worry-Free Business Security Advanced Ports* on page 4-9 for information on listening ports and see your firewall documentation for details on how to configure exception lists).

## Information to Prepare Before Performing the Installation

The installer will prompt you for the following information during installation:

- **Security Server details.** The domain/hostname or the IP address of the security server and the target directory where Worry-Free Business Security Advanced installs the security server files.

- **Proxy server details.** If a proxy server handles Internet traffic on your network, you must configure proxy server information (if required, the user name and password too). This information is necessary to download the latest components from the Trend Micro update server. You can enter proxy server information during or after installation. Use the Web console to enter information after installation.
- **SMTP server.** If using an SMTP server to send notifications, enter the name of the SMTP server, the port number, and the sender's and recipients' email addresses.

---

**Note:** If the SMTP server is on the same computer as Worry-Free Business Security Advanced and is using port 25, the installation program detects the name of the SMTP server and updates the **SMTP Server** and **Port** fields.

---

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

---

**WARNING!** *If you are installing the Messaging Security Agent on a server that is running lockdown tools (such as typically implemented for Windows 2000 server with IIS 5.0), remove the lockdown tool so that it does not disable the IIS service and causes the installation to fail.*

---

## Understanding Worry-Free Business Security Advanced Ports

Worry-Free Business Security Advanced utilizes two types of ports:

- **Server listening port (HTTP port).** Used to access the Trend Micro Security Server. By default, Worry-Free Business Security Advanced uses one of the following:
  - **IIS server default Web site.** The same port number as your HTTP server's TCP port.
  - **IIS server virtual Web site.** 8059
  - **Apache server.** 8059
- **Client listening port.** A randomly generated port number through which the Client receives commands from the Trend Micro Security Server.

You can modify the server listening port during or after the installation. You can modify the Client listening port only during installation.

---

**WARNING!** *Many hacker and virus attacks use HTTP and are directed at ports 80 and/or 8080– commonly used in most organizations as the default Transmission Control Protocol (TCP) ports for HTTP communications.*
*If your organization is currently using one of these ports as the HTTP port, Trend Micro recommends using another port number.*

---

## Trend Micro Security Server Prescan

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

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

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

### Actions for Prescan Detections

If the Worry-Free Business Security Advanced setup program detects viruses, Trojans, or other potentially malicious code, you can take the following actions:

- **Clean.** Cleans an infected file by removing the virus or malicious application. Worry-Free Business Security Advanced encrypts and renames the file if the file is uncleanable.
- **Rename.** Encrypts the file and changes the file extension to VIR, VIR1, VIR2, and so on. The file remains in the same location. Refer to the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide* to decrypt a file encrypted by Worry-Free Business Security Advanced.
- **Delete.** Deletes the file.
- **Pass.** Does nothing to the file.

**Tip:** Trend Micro recommends cleaning or deleting infected files.

## Other Installation Notes

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

**WARNING!** *Make sure that you do not install the Web server on a computer that is running applications that might lock IIS. This could prevent successful installation. See your IIS documentation for more information.*

**Tip:** Trend Micro recommends installing Worry-Free Business Security Advanced during non-peak hours to minimize the effect on your network.

# Worry-Free Business Security Advanced Installation Methods

There are three methods for installing Worry-Free Business Security Advanced:

- **Typical.** Provides a simple and easy solution for installing Worry-Free Business Security Advanced using Trend Micro default values. This method is suitable for a small business using a single Trend Micro Security Server and up to ten Clients.
- **Custom**. Provides flexibility in implementing your network security strategy. This method is suitable if you have many computers and servers or multiple Exchange servers.
- **Silent**. Performing a Silent installation creates a record file that you can use to perform identical installations on other computers or networks.

---

**Tip:** You can preserve your Client settings when you upgrade to this version of Worry-Free Business Security Advanced or if you need to reinstall this version of the Worry-Free Business Security Advanced. See *Upgrading from a Previous Version* on page 5-2 for instructions.

---

**Note:** If information from a previous MSA installation exists on the Client, you will be unable to install MSA successfully. Use the Windows Installer Cleanup Utility to clean up remnants of the previous installation. To download the Windows Installer Cleanup Utility, visit:
**http://support.microsoft.com/kb/290301/en-us**

---

# Performing a Typical Installation

The Typical installation method follows the same flow as the Custom installation method (refer to *Performing a Custom Installation* on page 4-13). During a Typical installation the following options are not available because they use the Trend Micro default settings:

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

- **Web server settings**
  - **Web Site.** OfficeScan
  - **Default URL.** `https://<IP_ADDRESS>:4343/SMB`
- **Client/Server Security Agent settings.** Refer to the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide* for information.

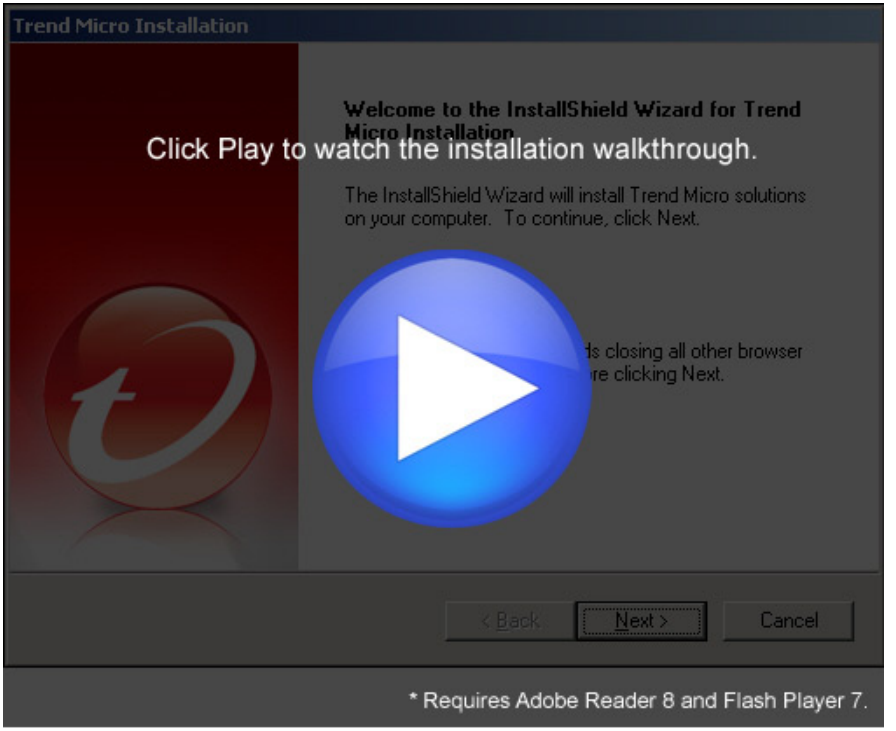



**FIGURE 4-1. Installation walkthrough**

To perform an installation using the Typical method follow the steps in *Performing a Custom Installation* on page 4-13 ignoring the steps that are relevant to Custom Installation.

# Performing a Custom Installation

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

1. Perform pre-configuration tasks. Refer to *Part 1: Pre-configuration Tasks* on page 4-13.
2. Enter the settings for the Trend Micro Security Server and Web console. Refer to *Part 2: Configuring the Security Server and Web Console Settings* on page 4-19.
3. Configure the Client/Server Security Agent and Messaging Security Agent installation options. Refer to *Part 3: Configuring the Client/Server Security Agent and Messaging Security Agent Installation Options* on page 4-31.
4. Start the installation process. Refer to *Part 4: Installation Process* on page 4-36.
5. **Optional.** Configure the Remote Messaging Security Agent installation option for remote Exchange servers. Refer to *Part 5: Starting the Remote Messaging Security Agent Installation* on page 4-37.

## Part 1: Pre-configuration Tasks

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

---

**Tip:** Close any running applications before installing Worry-Free Business Security Advanced. If you install while other applications are running, the installation process may take longer to complete.

---

**To start the pre-configuration tasks:**

1. Open the folder that contains the setup files and double-click the `SETUP.EXE` file. The **Trend Micro Installation** screen appears.

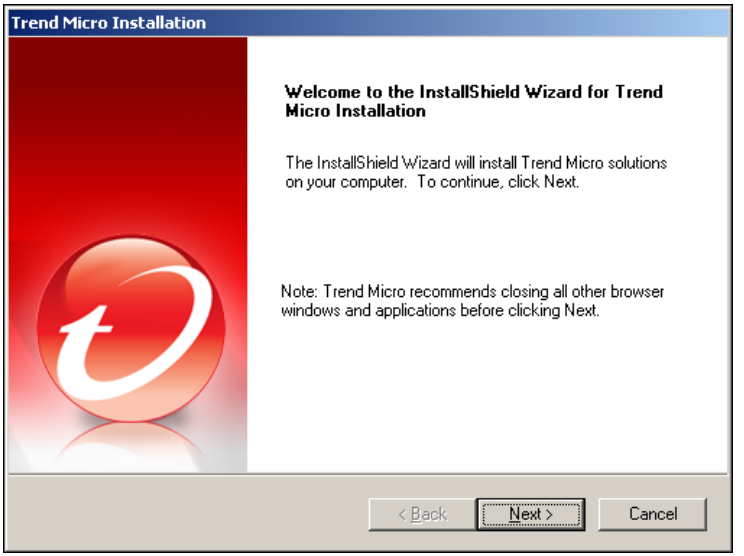



**FIGURE 4-2. Worry-Free Business Security Advanced Welcome screen**

2. Click **Next**. The **License Agreement** screen appears.
3. Read the license agreement. If you agree with the terms, select **I accept the terms of the license agreement**.
4. Click **Next**. The **Product Activation** screen appears.


**FIGURE 4-3. Product Activation screen**

5. From the **Setup Type** screen, choose one of the following options and click **Next**:

   - **Full Version**
   - **Evaluation Version with Email Reputation Services.** Refer to:

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

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

---

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

---

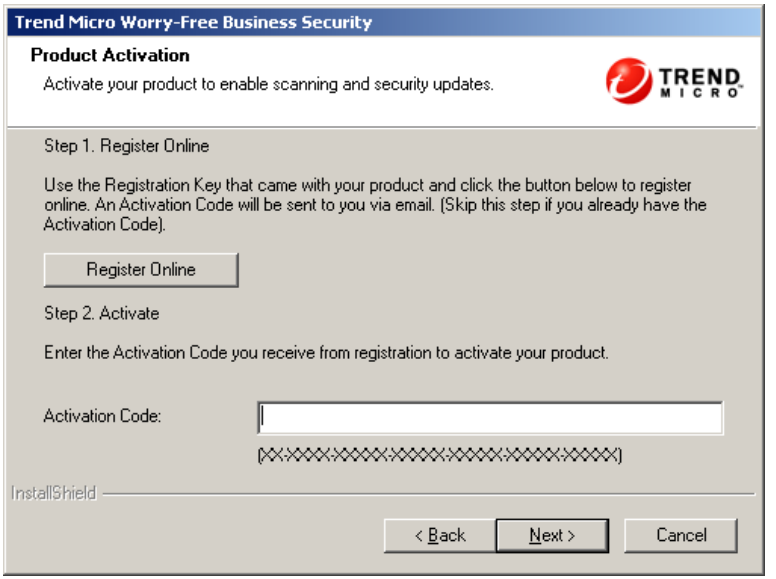



**FIGURE 4-4. Product Activation screen**

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

---

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

---

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

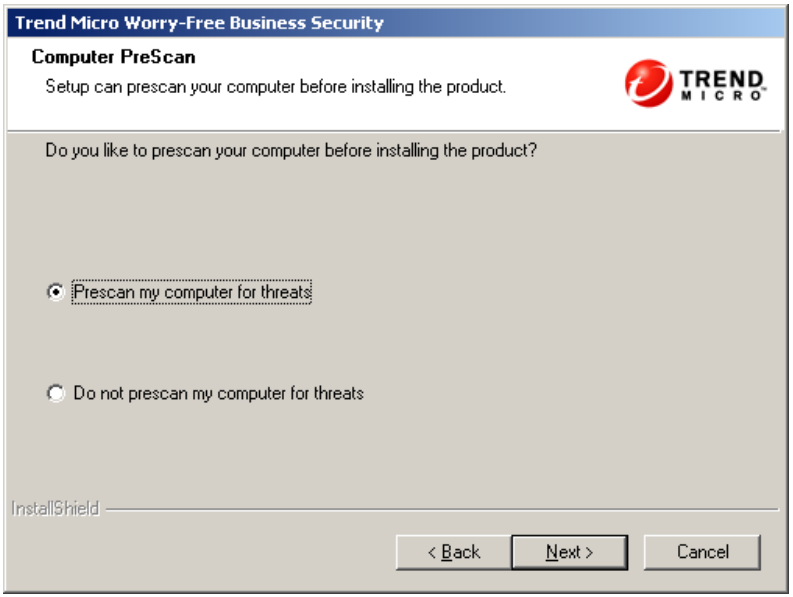



**FIGURE 4-5. Computer Prescan screen**

9. Choose whether to prescan your computer for threats by selecting one of the following options:
   - **Prescan my computer for threats**
   - **Do not prescan my computer for threats**

---

**Note:** If you choose to prescan your computer for threats, a threat progress screen will appear while scanning is taking place. See *Actions for Prescan Detections* on page 4-10.

---

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

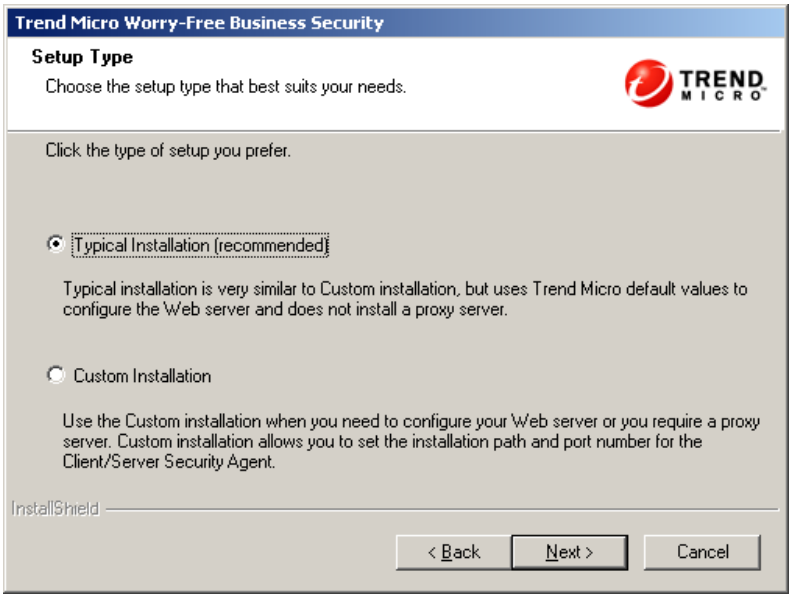



**FIGURE 4-6. Setup Type screen**

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

    Refer to *Worry-Free Business Security Advanced Installation Methods* on page 4-11 for the differences.

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

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

    This completes all pre-installation tasks.

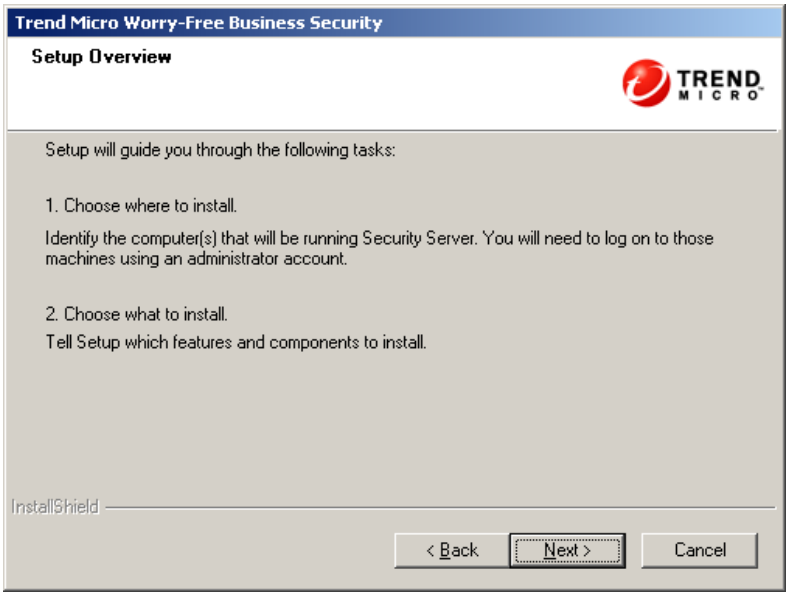



**FIGURE 4-7. Installation Setup Overview screen**

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

## Part 2: Configuring the Security Server and Web Console Settings

**To configure the Security Server and Web console:**

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


**FIGURE 4-8. Security Server Installation Stage screen**

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

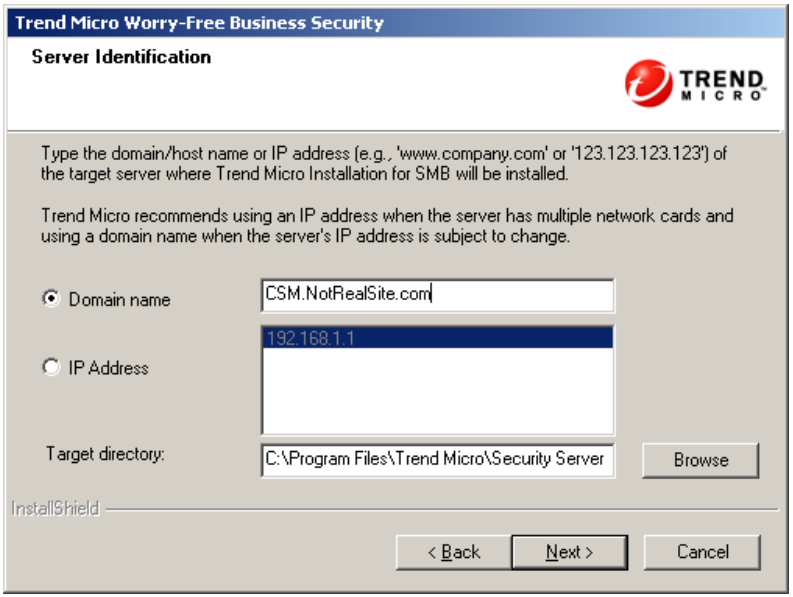



**FIGURE 4-9. Server Identification screen**

3. Choose from one of the following server identification options for client-server communication:

   - **Server information.** Choose Domain name or IP address:
     - **Domain name.** Verify the target server's domain name. You can also use the server's fully qualified domain name (FQDN) if necessary to ensure successful client-server communication.
     - **IP address.** Verify that the target server's IP address is correct.

---

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

---

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

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

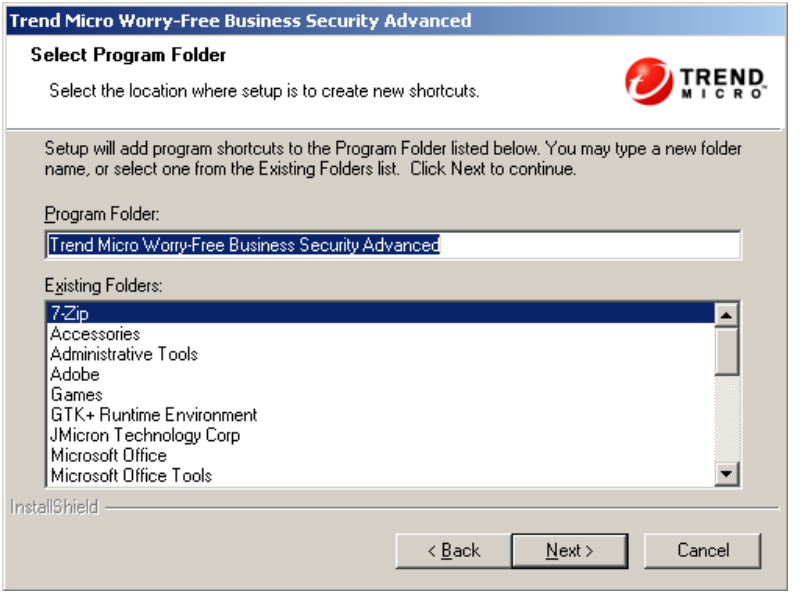



**FIGURE 4-10. Select Program Folder screen**

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

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


**FIGURE 4-11. Web Server screen**

---

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

---

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

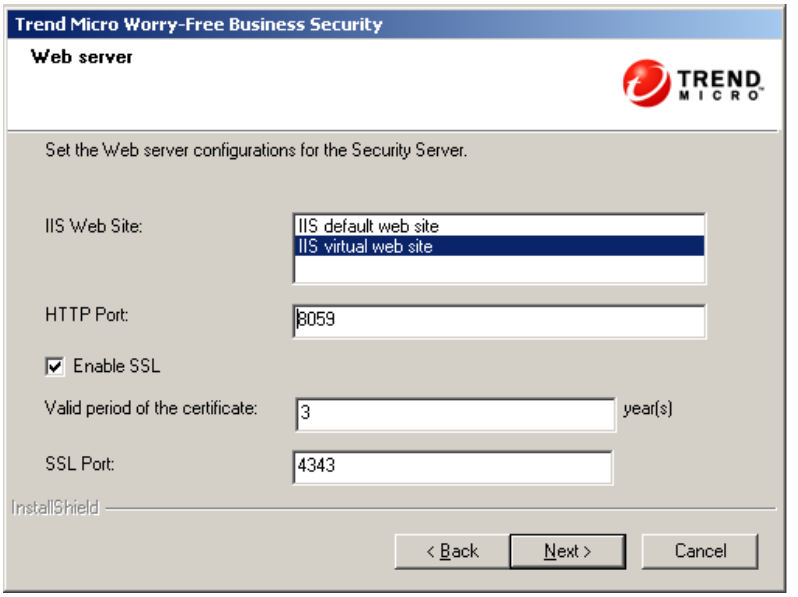



**FIGURE 4-12. IIS Web Server Configuration screen**

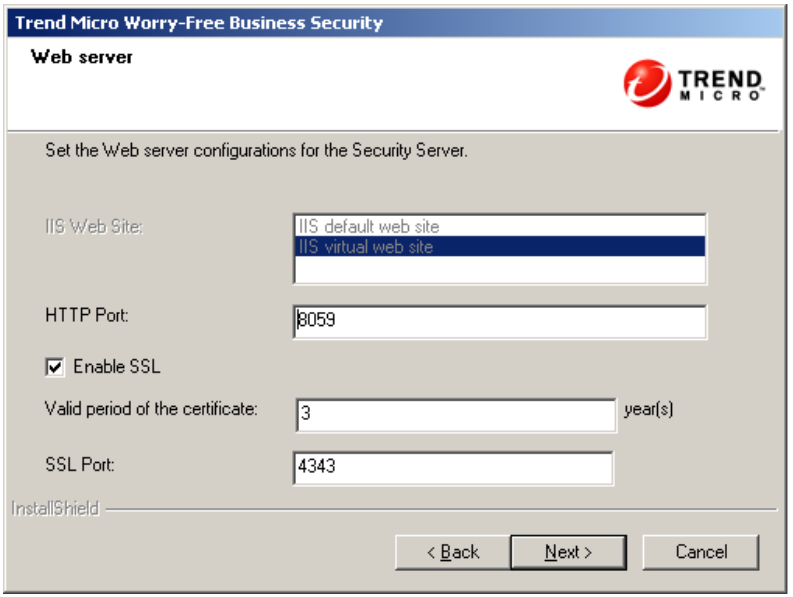



**FIGURE 4-13. Apache Web Server Configuration screen**

---

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

---

9. Configure the following Web server settings:
   - **HTTP port**
   - **Enable SSL**
   - **SSL port**

---

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

---

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

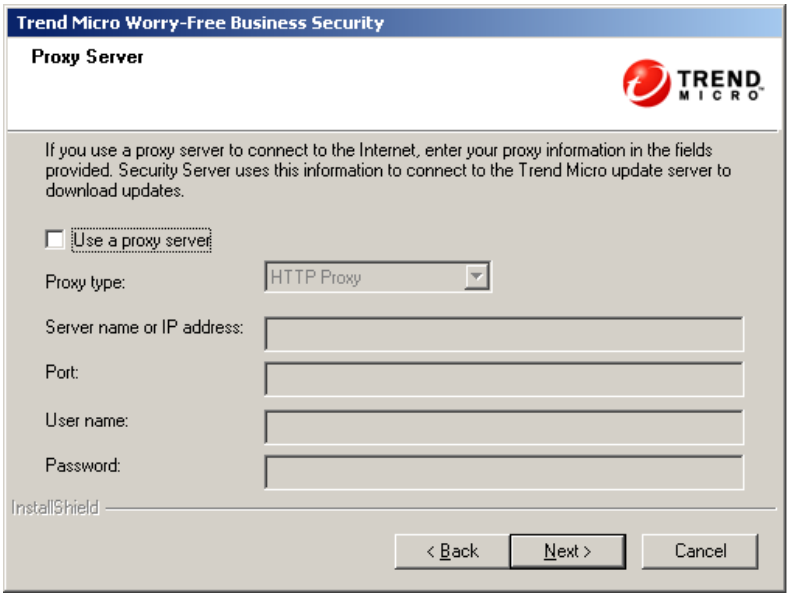



**FIGURE 4-14. Proxy Server screen**

---

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

---

11. If a proxy server is required to access the Internet, select the **Use a proxy server** check box and then provide the following information:
    - **Proxy type**
    - **Server or IP address**
    - **Port**
    - **User name**. Provide only if the server requires authentication.
    - **Password**. Provide only if the server requires authentication.
12. Click **Next**. The **SMTP Server and Notification Recipient(s)** screen appears.

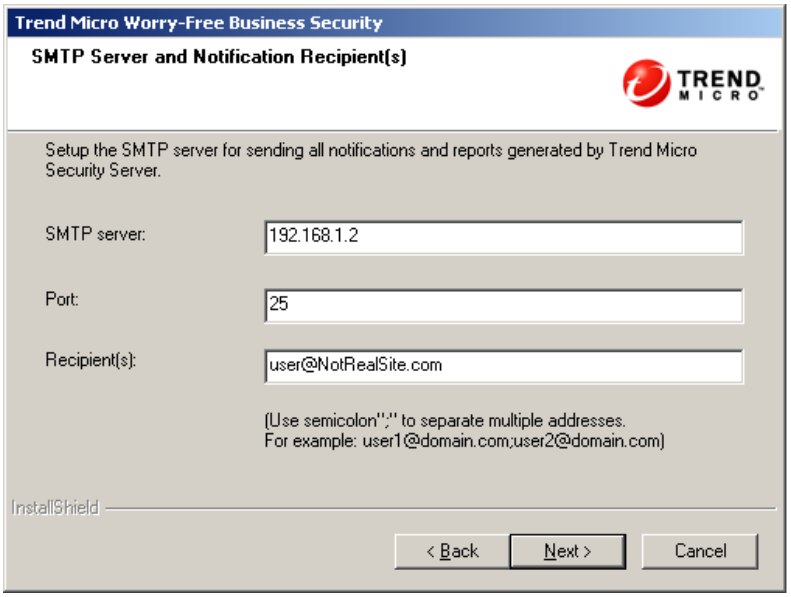



**FIGURE 4-15. SMTP Server and Notification Recipient(s) screen**

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

**Note:** If the SMTP server is on the same computer as Worry-Free Business Security Advanced and is using port 25, the installation program detects the name of the SMTP server and updates the **SMTP Server** and **Port** fields.

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

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

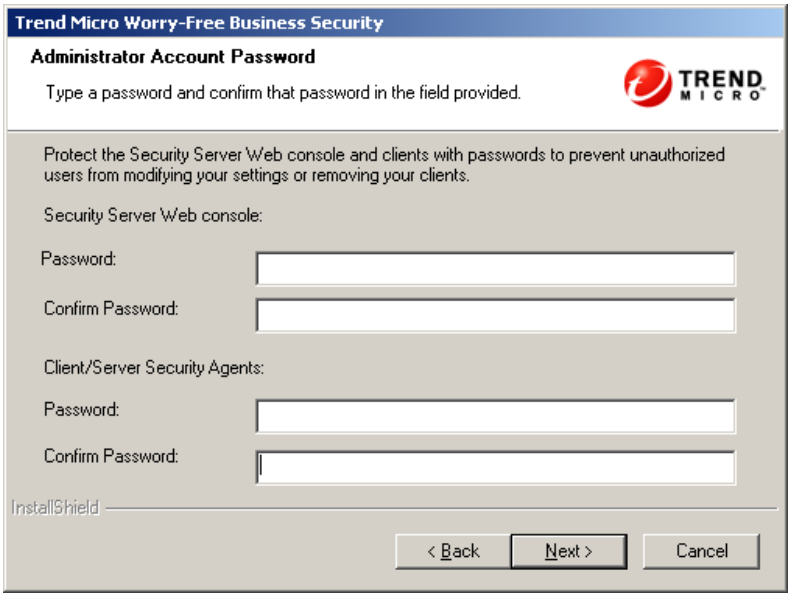



**FIGURE 4-16. Administrator Account Password screen**

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

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

16. Click **Next**. The **World Virus Tracking Program** screen appears.

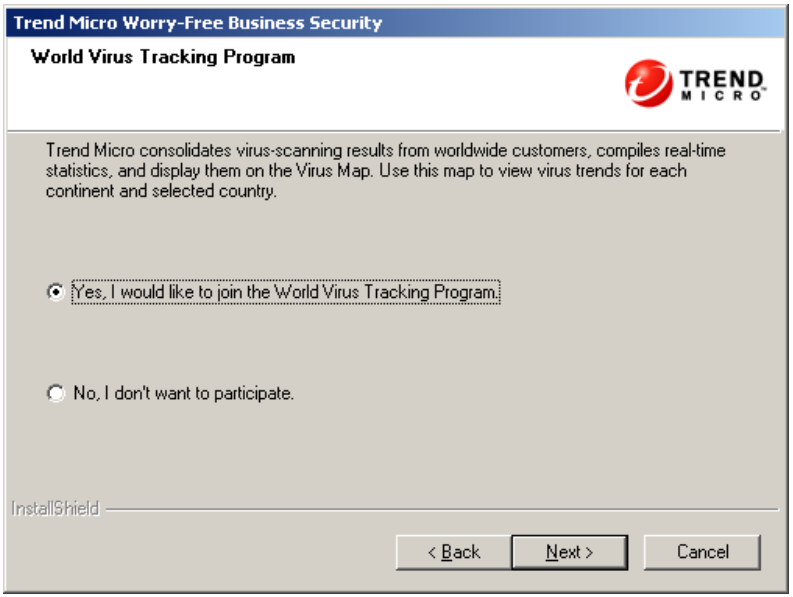



**FIGURE 4-17. World Virus Tracking Program screen**

17. Choose whether to participate in the World Virus Tracking Program.

    Trend Micro consolidates virus-scanning results from worldwide customers and uses this information to analyze worldwide virus trends in real time and to predict virus outbreaks and prevent them proactively.

18. Click **Next**. The **Component Selection** screen appears.

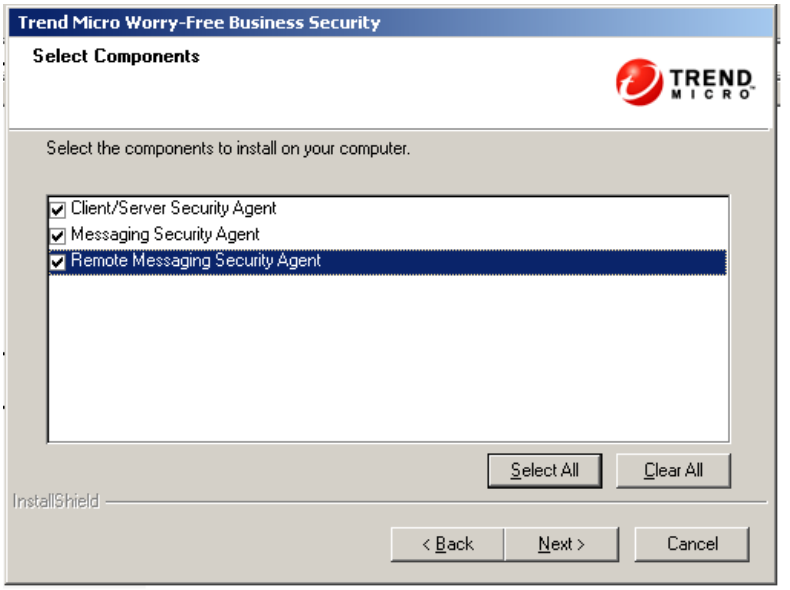



**FIGURE 4-18. Component Selection screen**

**19.** Select the components to install.

- Client/Server Security Agent
- Messaging Security Agent
- Remote Messaging Security Agent

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


**FIGURE 4-19. Messaging Security Agent Installation Stage screen**

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

## Part 3: Configuring the Client/Server Security Agent and Messaging Security Agent Installation Options

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

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

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

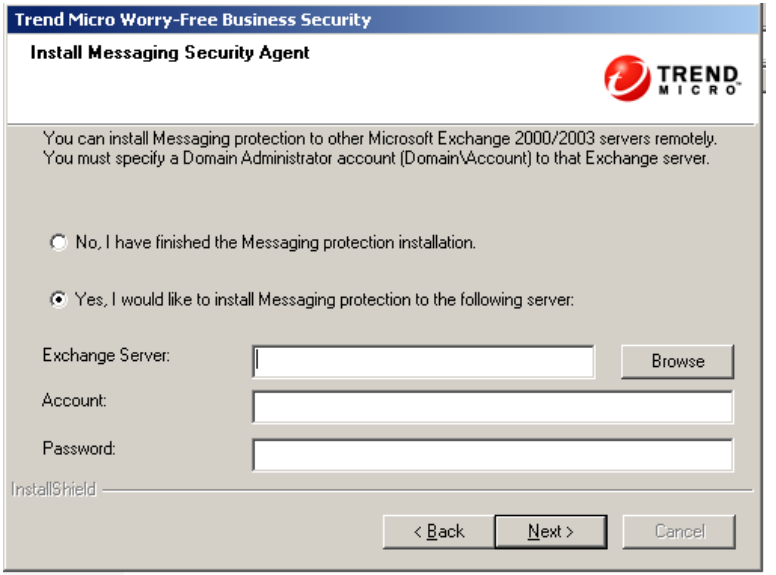



**FIGURE 4-20. Install Messaging Security Agent screen**

2. Enter the Domain Administrator account information.
   - **Account**
   - **Password**

---

**Note:** The installation program will automatically detect the name of the local Exchange server and fill in the **Exchange Server** field if the Exchange server is on the same computer as the Security Server.

---

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

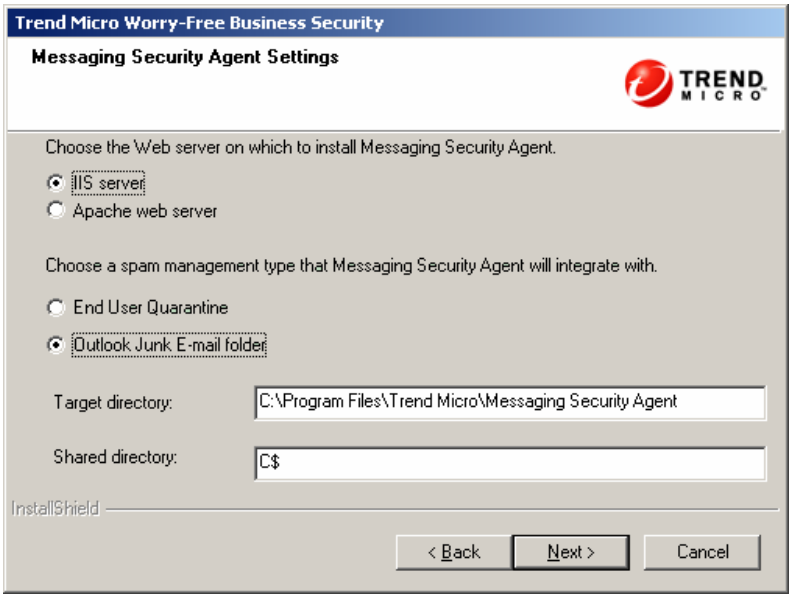



**FIGURE 4-21. Messaging Security Agent Settings screen**

---

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

---

4. From the Messaging Security Agent **Settings** screen:

   a. **Web server.** Select the type of Web server for hosting the Web console.

      - **IIS server**
      - **Apache web server**

   b. **Target directory.** Directory where Worry-Free Business Security Advanced installs the Messaging Security Agent files.

   c. **Shared directory.** System root directory for the Messaging Security Agent installation.

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

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


**FIGURE 4-22. Client/Server Security Agent Installation Stage screen**

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

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

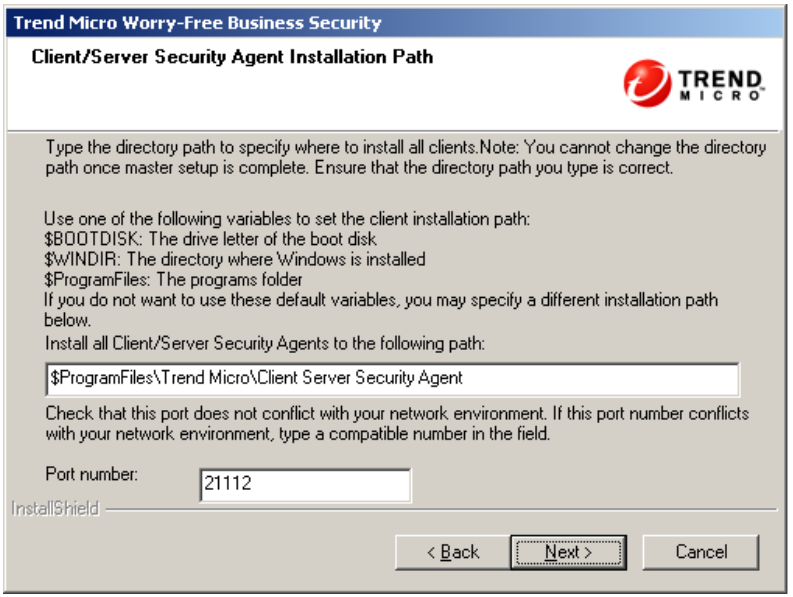



**FIGURE 4-23. Client/Server Security Agent Installation Path screen**

---

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

---

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

---

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

---

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

# Part 4: Installation Process

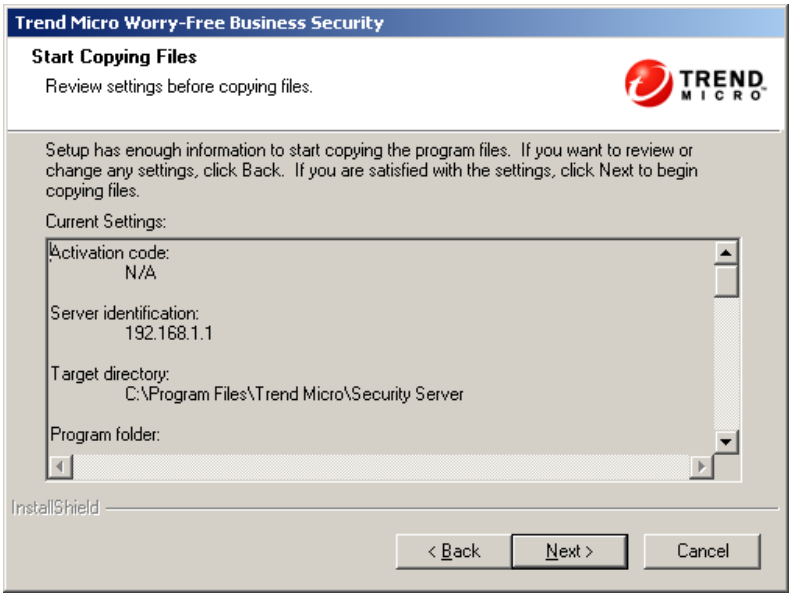



**FIGURE 4-24. Start Copying Files screen**

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

---

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

---

## Part 5: Starting the Remote Messaging Security Agent Installation

**To install the Remote Messaging Security Agent:**

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


**FIGURE 4-25. Remote Messaging Security Agent Installation Stage**

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

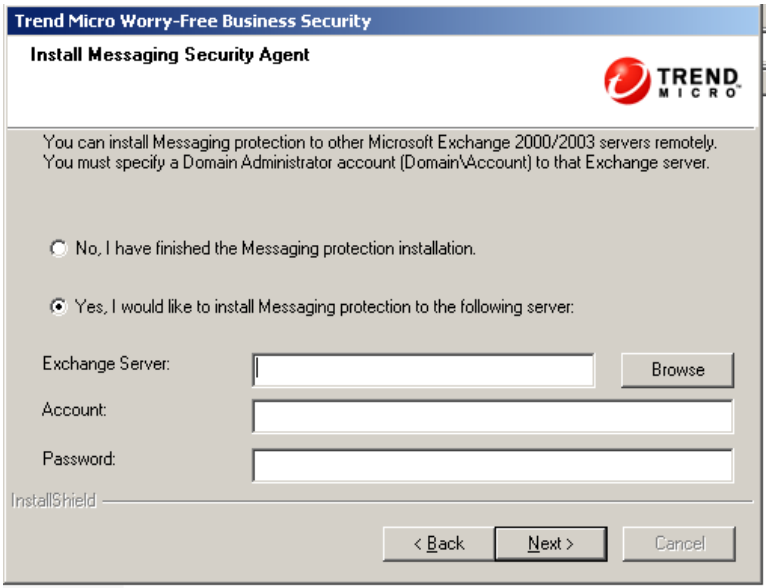



**FIGURE 4-26. Install Messaging Security Agent screen**

3. To install messaging protection to a remote Exchange server, click **Yes** and then enter credentials for an account with the domain administrator privileges.
   - **Exchange Server**. IP address or machine name
   - **Account**
   - **Password**

---

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

---

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

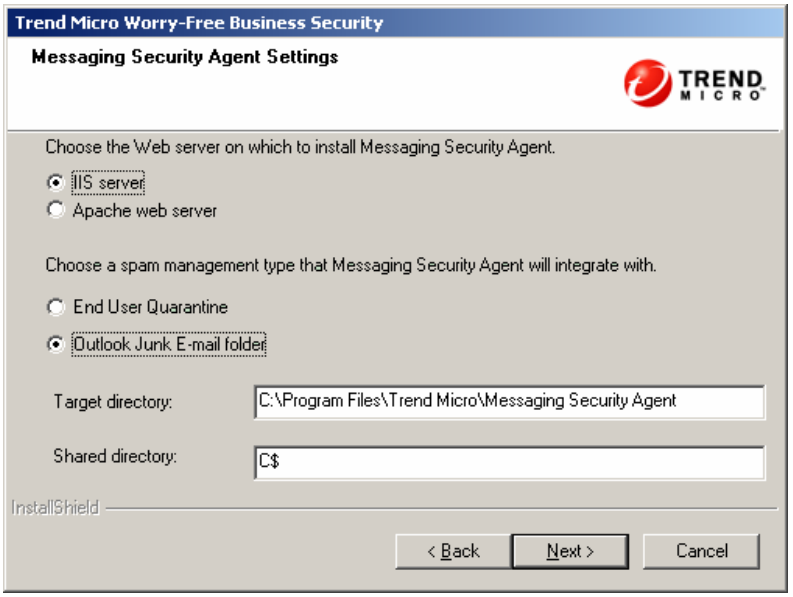



**FIGURE 4-27. Messaging Security Agent Settings screen**

---

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

---

5. From the Remote Messaging Security Agent Settings screen, update the following as required:

   - **Web server**
     - **IIS server**
     - **Apache Web server**
   - Spam management
     - **End User Quarantine**
     - **Outlook Junk E-mail folder**
   - **Target directory.** Directory where the Remote Messaging Security Agent files are installed.

- **Shared directory.** System root directory for the Remote Messaging Security Agent installation.

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

# Performing a Silent Installation

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

**Pre-configuration steps:**

1. In the command prompt, go to the directory where the Worry-Free Business Security Advanced setup files are located.
2. At the prompt, type **setup -r**.
3. To continue with the setup process and to learn more about configuring Worry-Free Business Security Advanced during installation see *Performing a Custom Installation* on page 4-13.
4. A confirmation message is displayed at the end of the installation.

**Starting the silent installation:**

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

To verify that the installation is successful, go to the Worry-Free Business Security Advanced folder and view the `setup.log` file. If `ResultCode=0`, the installation was successful.

# Verifying the Installation

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

**To verify the installation:**

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

  **`https://{Worry-Free Business Security Advanced_server_name}:{port number}/SMB`**

  If you are NOT using SSL, type `http` instead of `https`.

Chapter 5

# Upgrading/Migrating Worry-Free Business Security Advanced Security

This chapter includes the following topics:

# Upgrading from a Previous Version

The upgrade procedure is similar to the normal installation process except you type your existing Security Server when asked to identify the Security Server (domain name or IP address). Client/Server Security Agents and Messaging Security Agents will upgrade automatically. See *Worry-Free Business Security Advanced Installation Methods* on page 4-11.

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

**TABLE 5-1. Product Versions**

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

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

## Supported Upgrades

Worry-Free Business Security Advanced supports upgrades from any of the following versions:

- Upgrade from Client Server Messaging Security 3.5 to Worry-Free Business Security Advanced 5.0
- Upgrade from Client Server Messaging Security 3.6 to Worry-Free Business Security Advanced 5.0

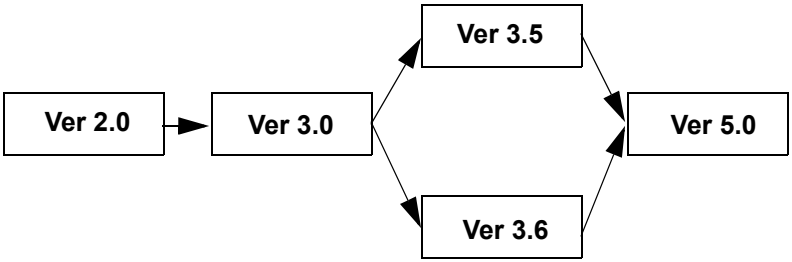



**FIGURE 5-1. Supported Upgrade Paths for Worry-Free Business Security Advanced 5.0**

## Unsupported Upgrades

Worry-Free Business Security Advanced 5.0 does not support upgrades under the following conditions:

- Upgrade from Client/Server Suite 2.0
- Upgrade from Client/Server/Messaging Suite 2.0
- Upgrade from OfficeScan Enterprise Edition or ScanMail for Microsoft Exchange
- Upgrade from Client/Server Security 3.0
- Upgrade from Client/Server/Messaging Security 3.0
- Upgrade from one language to another

## Before You Upgrade

You can preserve your Client settings when you upgrade to the newest version of Worry-Free Business Security Advanced. To ensure that you can easily restore your existing settings if the upgrade is unsuccessful, Trend Micro recommends backing up your Security Server database.

**To back up the Security Server database:**

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

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

**To delete log files:**

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

# Upgrading from an Evaluation Version

When your evaluation version is about to expire, a notification message displays on the **Live Status** screen. You can upgrade from an evaluation version to the fully-licensed version using the Web console. Your configuration settings will be saved. When you purchase a fully-licensed version, you will be given a Registration Key or an Activation Code.

**To upgrade from an evaluation version:**

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

---

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

---

# Migrating from Other Antivirus Applications

Worry-Free Business Security Advanced supports migration from other Antivirus applications. Worry-Free Business Security Advanced can automatically migrate the client software, but cannot uninstall the server application.

## Migrating from Trend Micro Anti-Spyware

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

- If you install the Worry-Free Business Security Advanced server on the same server as the TMASY server, the Worry-Free Business Security Advanced server setup program will *not* remove or upgrade the TMASY server. You need to manually remove the TMASY server before installing the Worry-Free Business Security Advanced server on the same machine.
- Removing the TMASY client before installing the Client/Server Security Agent is not required. The Client/Server Security Agent setup program will automatically remove the TMASY client when detected on the same client computer and then install Client/Server Security Agent.
- The anti-spyware settings for Client/Server Security Agent and TMASY are different. After installing the Client/Server Security Agents, you may need to configure the anti-spyware settings to make them the same as your previous TMASY client settings. Refer to Table 5-2 for a comparison of the Client/Server Security Agent and TMASY anti-spyware settings.

**TABLE 5-2. Comparison of Client/Server Security Agent and TMASY Anti-Spyware Settings**

| | Client/Server Security Agent | Trend Micro Anti-Spyware Client |
|---|---|---|
| **Real-time Scan** | Enabled | Disabled (Active Application Monitoring) |
| Default action | Clean | Deny executable |
| **Manual Scan** | | |
| Scan type | Full scan | Quick scan |
| Default action | Clean | Scan and do nothing (auto clean is disabled by default) |
| Scan on start | N/A | Enabled |
| Check network | N/A | Enabled |
| **Scheduled Scan** | Disabled | Enabled |
| Scan schedule | Every Monday | Daily |
| Scan time | 12:30 | 23:00 |
| Scan type | Full scan | Quick scan |
| Default action | Clean | Scan and do nothing (auto clean is disabled by default) |

## Migrating from Other Antivirus Applications

Migrating from other antivirus software to Worry-Free Business Security Advanced is a two-step process: the installation of the Trend Micro Security Server, followed by the automatic migration of the Clients.

Automatic client migration refers to replacing existing client antivirus software with the Client/Server Security Agent program. The client setup program automatically removes the other antivirus software on your client computers and replaces it with the Client/Server Security Agent.

Refer to Table 5-3 for a list of client applications that Worry-Free Business Security Advanced can automatically remove.

**Note:** Worry-Free Business Security Advanced only removes the following client installations, not server installations.

**TABLE 5-3. Removable Antivirus Applications**

| **Trend Micro** | | |
|---|---|---|
| • OfficeScan 95 client 3.5<br>• OfficeScan NT client version 3.1x<br>• OfficeScan NT client version 3.5<br>• PccillinCorp 95 client<br>• PccillinCorp NT client<br>• ServerProtect for Windows NT<br>• Trend Micro PC-cillin 2004 (AV)<br>• Trend Micro PC-cillin 2004 (TIS)<br>• Trend PC-cillin 2000 7.61(WinNT)<br>• Trend PC-cillin 2000(Win9X) | • Trend PC-cillin 2000(WinNT)<br>• Trend PC-cillin 2002<br>• Trend PC-cillin 2003<br>• Trend PC-cillin 6<br>• Trend PC-cillin 95 1.0<br>• Trend PC-cillin 95 1.0 Lite<br>• Trend PC-cillin 97 2.0<br>• Trend PC-cillin 97 3.0<br>• Trend PC-cillin 98<br>• Trend PC-cillin 98 Plus(Win95)<br>• Trend PC-cillin 98 Plus(WinNT)<br>• Trend PC-cillin NT | • Trend PC-cillin NT 6<br>• Virus Buster 2000<br>• Virus Buster 2000 for NT ver.1.00<br>• Virus Buster 2000 for NT ver.1.20<br>• Virus Buster 2001<br>• Virus Buster 98<br>• Virus Buster 98 for NT<br>• Virus Buster NT<br>• VirusBuster 95 1.0<br>• VirusBuster 97<br>• VirusBuster 97 LiteOfficeScan 95 client 3.1x<br>• VirusBuster Lite 1.0<br>• VirusBuster Lite 2.0 |
| **Symantec™** | | |
| • Norton AntiVirus 2.0 NT<br>• Norton AntiVirus 2000 9X<br>• Norton AntiVirus 2000 NT<br>• Norton AntiVirus 2001 9X<br>• Norton AntiVirus 2001 NT<br>• Norton AntiVirus 2002 NT<br>• Norton AntiVirus 2003<br>• Norton AntiVirus 5.0 9X<br>• Norton AntiVirus 5.0 NT<br>• Norton AntiVirus 5.31 9X<br>• Norton AntiVirus 5.31 NT<br>• Norton AntiVirus 5.32 9X<br>• Norton AntiVirus 5.32 NT | • Norton AntiVirus 5.31 NT<br>• Norton AntiVirus 5.32 9X<br>• Norton AntiVirus 5.32 NT<br>• Norton AntiVirus 6.524<br>• Norton AntiVirus 7.0 9X<br>• Norton AntiVirus 7.0 NT<br>• Norton AntiVirus 7.5 9X<br>• Norton AntiVirus 7.5 NT<br>• Norton AntiVirus 8.0 9x<br>• Norton AntiVirus 8.0 NT<br>• Norton Antivirus™ CE 10.0<br>• Norton Antivirus™ CE 10.1<br>• Norton Antivirus™ CE 6.524 | • Norton Antivirus™ CE 7.0 for Windows NT<br>• Norton Antivirus™ CE 7.0 NT<br>• Norton Antivirus™ CE 7.5 9x<br>• Norton Antivirus™ CE 7.5 NT<br>• Norton Antivirus™ CE 8.0 9x<br>• Norton Antivirus™ CE 8.0 NT<br>• Norton Antivirus™ CE 8.1 server<br>• Norton Antivirus™ CE 9.0 |

**TABLE 5-3. Removable Antivirus Applications**

| | | |
|---|---|---|
| **McAfee™** | | |
| • Dr Solomon 7.77,7.95 NT<br>• Dr.Solomon 4.0.3<br>• Dr.Solomon 4.0.3 NT<br>• ePOAgent1000<br>• ePOAgent2000<br>• McAfee NetShield 4.5<br>• McAfee NetShield NT 4.03a | • McAfee VirusScan 4.5<br>• McAfee VirusScan 4.51<br>• McAfee VirusScan 6.01<br>• McAfee VirusScan 95(1)<br>• McAfee VirusScan 95(2)<br>• McAfee VirusScan ASaP | • McAfee VirusScan Enterprise 7<br>• McAfee VirusScan NT<br>• McAfee VirusScan TC<br>• McAfee VirusScan(MSPlus98)<br>• V3Pro 98 |
| **LANDesk™** | | |
| • LANDesk VirusProtect5.0 | | |
| **Computer Associates™** | | |
| • CA InocuLAN_NT 4.53<br>• CA InocuLAN_9.x 4.53 | • CA eTrust InoculateIT 6.0 | • CA InocuLAN 5 |
| **Ahnlab™** | | |
| • V3Pro 2000 Deluxe | • V3Pro 98 Deluxe | |
| **Panda Software™** | | |
| • Panda Antivirus Local Networks | • Panda Antivirus 6.0 | • Panda Antivirus Windows NT WS |
| **F-Sercure™** | | |
| • F-Secure 4.04<br>• F-Secure 4.08, 4.3 5.3 | • F-Secure BackWeb | • F-Secure Management Agent |
| **Kaspersky™** | | |
| • Antivirus Personal 4.0, Workstation 3.5. 5.4 | | |
| **Sophos™** | | |
| • Sophos Anti-Virus NT | • Sophos Anti-Virus 9X | |
| **Authentium™** | | |
| • Command AV 4.64 9x | | |

**TABLE 5-3. Removable Antivirus Applications**

| | | |
|---|---|---|
| **Amrein™** | | |
| • Cheyenne AntiVirus 9X | • Cheyenne AntiVirus NT | |
| **Grisoft™** | | |
| • Grisoft AVG 6.0 | | |
| **Others** | | |
| • ViRobot 2k Professional | • Tegam ViGUARD 9.25e for Windows NT | |

# Upgrading the Client/Server Security Agent

You can upgrade to a full version of Worry-Free Business Security Advanced from a previous version or from a evaluation version. When you upgrade the Trend Micro Security Server, Clients are automatically upgraded.

Chapter 6

# Web Console Overview

This chapter describes the main features and elements Web console. It also discusses how to navigate the Dashboard.

The topics discussed in this chapter include:

# Exploring the Web Console

When you install the Trend Micro Security Server, you also install the Web console, which uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

**To open the Web console:**

1. On any computer on the network, open a Web browser and type the following in the address bar:

   `https://{`Worry-Free Business Security Advanced`_Server_Name}:{port number}/`SMB in the address bar.

   If you are NOT using SSL, type `http` instead of `https`.

   Refer to *System Requirements* on page 4-2 to view browser requirements.

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


**FIGURE 6-1. Log on screen of Worry-Free Business Security**

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

---

**Note:** You might be expected to install additional plugins. Click **Install** at the prompt.

---

# Getting Around the Web Console

After successfully logging on, the Web console appears. There are two main parts to the Web console: the main navigation menu and the main body frame. Some screens contain a side menu and a tool bar.

## Live Status

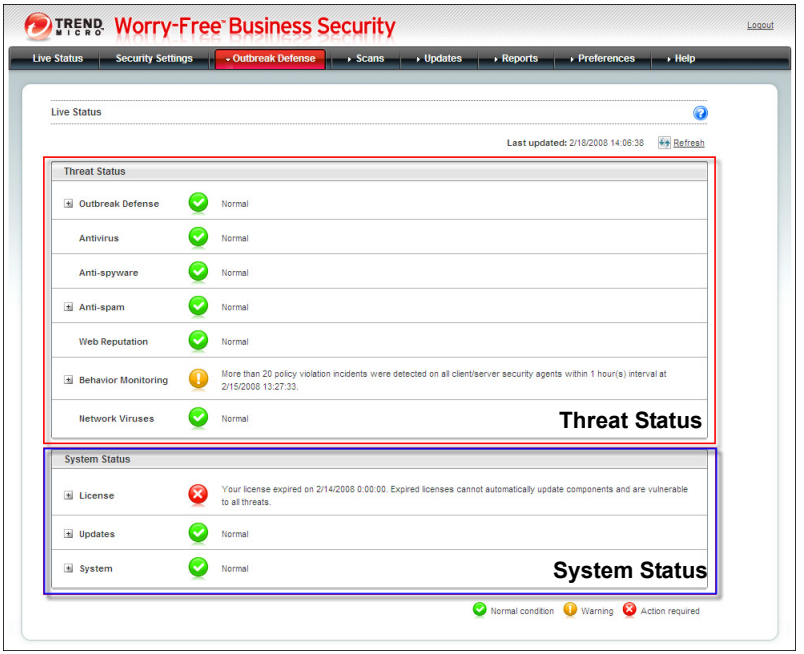



**FIGURE 6-2. Live Status screen**

The main navigation menu contains the following sections:

- **Threat Status.** View the latest threats to desktops, portable computers, servers, and Exchange servers.
- **System Status.** Monitor server disk space, deploy updates to vulnerable Clients, and view license information.

## Security Settings

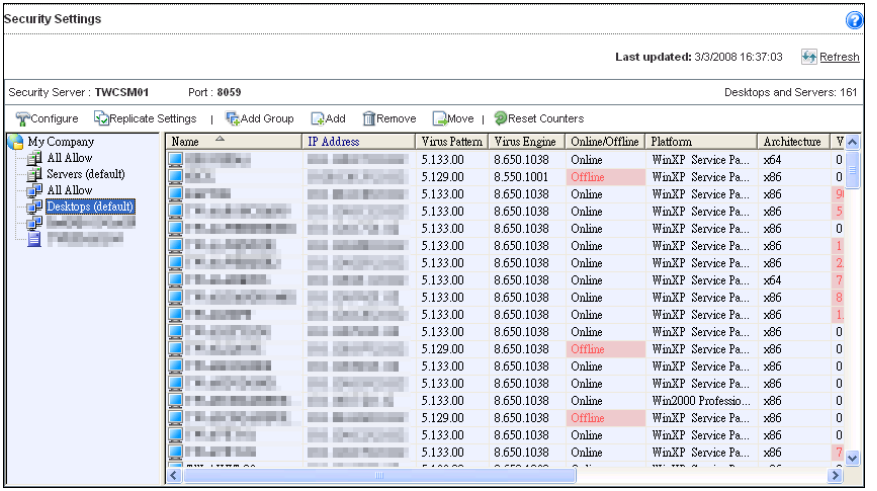



**FIGURE 6-3. Security Settings screen**

From the **Security Settings** screen, you can:

- Configure security setting for desktops, portable computers, servers, and Exchange servers
- Replicate settings from one group to another.
- Add Groups to the Security Server.
- Add computers to a Group.
- Remove computers from a Group.
- Move desktops/servers from one Security Server to another.
- Reset counters.

## Outbreak Defense

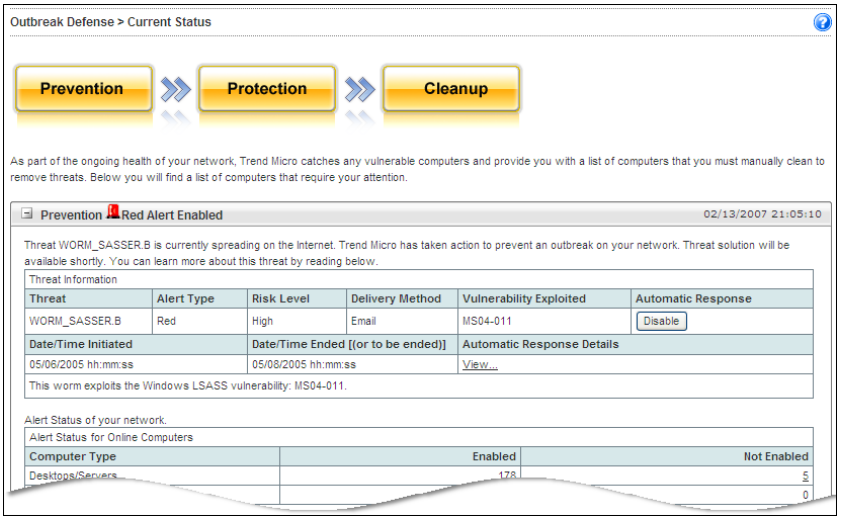



**FIGURE 6-4. Outbreak Defense > Current Status screen**

From the **Outbreak Defense** screen, you can:

- View recent virus outbreak activity.
- Scan desktops, portable computers, servers, and Exchange servers for vulnerabilities.
- View the vulnerability level of different desktops, portable computers, servers, and Exchange servers.
- Detect vulnerabilities on desktops, portable computers, servers, and Exchange servers.
- View and clean-up desktops, portable computers, servers, and Exchange servers that are infected with viruses or other malware.

## Scans


**FIGURE 6-5. Scans > Manual Scan screen**

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

- Scan desktops, portable computers, servers, and Exchange servers for malicious applications.
- Configure exclusions. Worry-Free Business Security Advanced will not scan these files or folders (can also be configured from **Security Settings**).
- Schedule scans of desktops, portable computers, servers, and Exchange servers.

## Updates

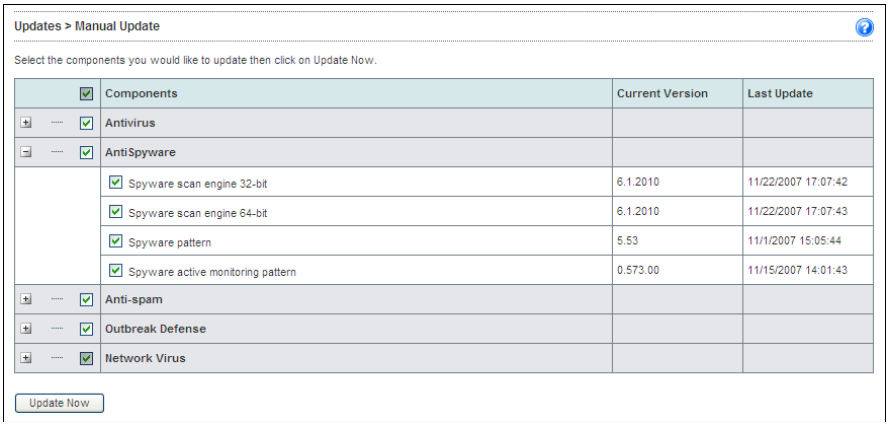



**FIGURE 6-6. Updates > Manual Update screen**

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

- Check the Trend Micro ActiveUpdate server for the latest updated components—Antivirus, Anti-Spyware, Anti-Spam, Outbreak Defense, and Network Virus pattern files.
- Configure update source.
- Configure update schedule.
- Assign and configure update Agents.

## Reports

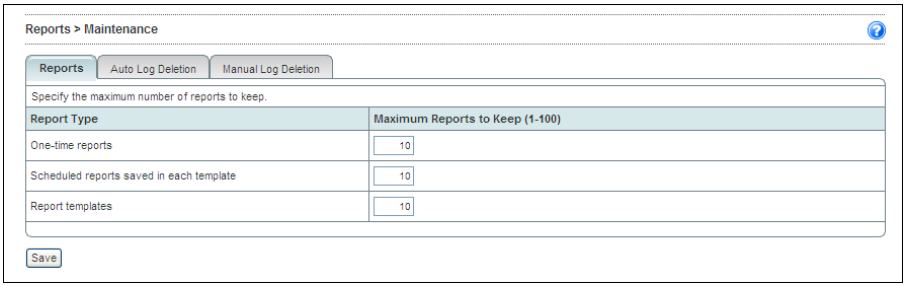



**FIGURE 6-7. Reports > Maintenance screen**

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

- Generate one-time reports.
- Configure scheduled reports.
- Query existing logs.
- Maintain and delete logs.

## Preferences

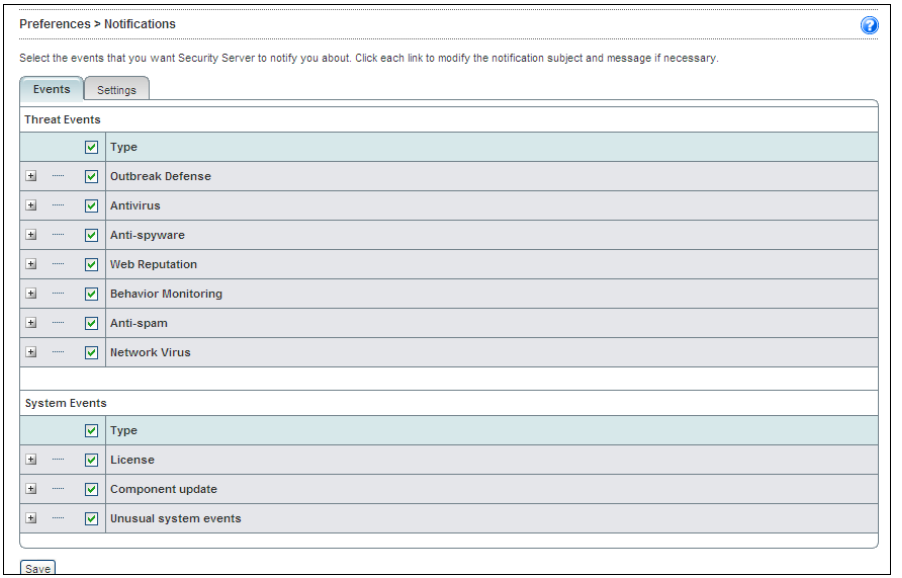



**FIGURE 6-8. Preferences > Notifications screen**

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

- Set up notifications for different events that occur.
- Configure global settings.
- Change the administrator password.
- Use different client and administrative tools to help manage security for the network and Clients.
- View product license information, maintain the administrator password, and help keep the global business environment safe by joining the World Virus Tracking program.
- Change World Virus Tracking Program participation.
- Manage the Plug-in Manager.

## Help

Use the help menu and/or the Administrator's Guide to get answers to Worry-Free Business Security Advanced questions, view other Trend Micro security solutions, and get customer support.

Chapter 7

# Configuring Security Settings

This chapter details the default settings and briefly describes the available configuration options. Refer to the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide* or the *Online Help* for detailed instructions.

The topics discussed in this chapter include:

# About Security Settings

Security settings determine the level of security enforced for a group of Clients. A Group in Worry-Free Business Security Advanced is a collection of Clients that share the same configuration and run the same tasks. A Worry-Free Business Security Advanced Group is different from a Windows domain. There can be several Worry-Free Business Security Advanced Groups in any given Windows domain.

---

**Note:** Administrator's can configure Clients only at the group level. To individually configure a Client, create a group and only that Client into the new group.

---

This guide gives a description of the key tasks. For more detailed information about how to customize these tasks, refer to Worry-Free Business Security Advanced 5.0 *Online Help* or Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide*.

# Configuring Desktop and Server Groups

**To set a task or configuration for a group of Clients:**

1. From the **Security Settings** screen, select the group of Clients from the Security Groups Tree.
2. Click **Configure**. A new menu appears on the left-hand side of the screen allowing you to set the tasks and configuration options for the group.
3. Click a configuration item from the sidebar menu on the left-hand side of the screen and update the settings as required. Refer to *Desktops/Server Settings* on page 7-2.

## Desktops/Server Settings

### Antivirus/Anti-Spyware

Real-time scanning is an ongoing scan that runs in the background. Whenever it detects a file containing an Internet threat, it performs the configured action against that threat and sends the information to the Security Server database to be included in

the logs. When enabled, Client/Server Security Agents can display alert messages, showing the name of the infected file and the threat name on a Client.

The speed of Real-time scanning depends on your settings. You can increase the performance of real-time scans by decreasing the number of files for scanning or by limiting the maximum number of compression layers to scan.

### Default Settings

- **Real-time scanning.** *Enabled* and scans *all incoming and outgoing files* on your Clients.
- **Files scanned.** IntelliScan uses Trend Micro recommended settings to optimize scanning speed.
- **Action on detected threats.** *Cleans* all detected files or *deletes* files that cannot be cleaned.
- **Advanced scanning options.** *Scans all compressed files* up to *2* compression layers deep.
- **Exclusions.** *Excludes* scanning folders where other Trend Micro products are installed.

## Firewall

Worry-Free Business Security Advanced includes a Firewall to screen some types of communications with the Internet. If you enable the Firewall, Trend Micro recommends the Simple mode for small and medium-sized businesses.

To customize your Firewall configuration, select **Advanced mode**. The Advanced mode is set to initially use the Trend Micro default configuration for **Simple mode**, but allows for greater control than **Simple mode**.

---

**WARNING!** *Trend Micro recommends uninstalling other software-based firewalls before deploying and enabling the Firewall. Multiple firewall installations on the same Client may produce unexpected results.*

---

### Default Settings

Firewall is disabled.

## Behavior Monitoring

Worry-Free Business Security Advanced can monitor unusual modifications to the operating system or on installed software. Administrators can also create exception lists. Exception lists include trusted and blocked software.

### Default Settings

Enabled

## TrendSecure

With TrendSecure tools, users can check the safety of a wireless connection, prevent key logging, and prevent Phishing incidents. Administrators can configure different settings depending on the location of the user.

### Default Settings

Disabled

## Client Privileges

Administrators can grant users privileges to modify individual scan settings and uninstall or unload Agents. Granting users privileges is a way of sharing control over individual Client/Server Security Agent settings.

However, to enforce uniform antivirus policy throughout your organization, Trend Micro recommends granting limited privileges to users. This ensures that end users do not modify the scan settings or remove the Client/Server Security Agent without permission.

### Default Settings

Only the following options are enabled by default:

- Allow users to configure proxy settings
- Perform “Update Now”
- Download from the Trend Micro ActiveUpdate Server
- Enable Scheduled Update
- Client Security: Normal

### Quarantine

When a Client/Server Security Agent detects files containing Internet threats, it quarantines the detected files to a folder on the Client. From this folder, the quarantined files are redirected to the Quarantine folder on the Security Server.

Define the location of the Quarantine folder on the Security Server by typing a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path in the **Quarantine Directory** screen.

#### Default Settings

The default directory on Clients is:

```
%Program Files%\Client Security Agent\SUSPECT
```

The default location of the Security Server quarantine folder is as follows:

```
Security Server\PCCSRV\Virus
```

# Configuring Exchange Servers

**To set a task or configuration for a group of Exchange servers:**

1. From the **Security Settings** screen, select the group of Exchange servers from the Security Groups Tree.
2. Click **Configure**. A new menu appears on the left-hand side of the screen allowing you to set the tasks and configuration options for the group.
3. Click a configuration item from the sidebar menu on the left-hand side of the screen and update the settings as required. Refer to *Exchange Servers Settings* on page 7-5.

## Exchange Servers Settings

### Antivirus

Real-time scanning is an ongoing scan that runs in the background. Whenever it detects an email message containing an Internet threat, it performs the user-configured action against that email message and sends the information to be included in the logs.

Messaging Security Agent scans the following in real time:

- All incoming and outgoing email messages
- SMTP messages arriving at the Exchange server from the Internet
- Public folder postings
- All server-to-server replications

### Default Settings

- **Real-time scanning.** *Enabled*; Real-time scanning scans all incoming and outgoing email messages on your Exchange servers
- **Files to scan.** *All scannable files*; scans all file attachments except those containing encrypted or password-protected files

> **Note:** Real-Time Scan will scan the encrypted or password-protected file only when a user decrypts the file.

- **Action on detected threats.** Performs a customized action for each type of threat:
  - For viruses, the action is *clean* (or *delete* entire message if *clean* is unsuccessful).

    Clean removes malicious code from infected message bodies and attachments. The remaining email message text, any uninfected attachments, and the cleaned attachments are delivered to the intended recipient(s).

  - For Trojans/worm, the action is *replace with text/file*. *Replace with text/file* deletes the infected content and replaces it with a text string or file.

    The email message is delivered to the intended recipient, but the text replacement informs them that the original content was infected and was replaced by a text string or a file.

  - *Delete entire message* for all messages that show a mass-mailing behavior.

    Mass-mailing behavior describes a situation when an infection spreads rapidly in an Exchange environment. The action set for mass-mailing behavior overrides all other actions.
- **Email message body.** *Includes* the body of email messages in the scan.
- **Very large messages.** *Excludes* email messages that exceed 30MB or contain attachments that exceed 30MB.

- **Compressed files.** *Excludes* compressed files when:
  - There are more than 9999 files in the compressed file.
  - When decompressed, the compressed file is larger than 100MB.
  - The file has more than five compression layers.

**Note:** To increase performance, Worry-Free Business Security Advanced does not clean infected files detected in compressed files and treats the files as uncleanable files. Real-time Scan will detect and clean the threat, if any, when extracted.

- **Password-protected, encrypted, or user-restricted files.** *Pass* action delivers these types of messages to the recipient.
- **Malicious macro code.** *Uses heuristic rules* to scan for malicious macro code and sets the detection level to *2*.

  Heuristic scanning is an evaluative method of detecting viruses. This method excels at detecting undiscovered viruses and threats, whose signatures have not been added to the virus pattern. A detection level of 2 is not too lenient or too restrictive. It detects most malicious macros without creating too many false positives.

**Tip:** Trend Micro recommends using **Exclusions** to set scanning restrictions to protect against Denial of Service (DoS) attacks. DoS attacks cause a loss of 'service', namely a network connection. Typically, DoS attacks negatively affect network bandwidth or overload computer resources such as memory. Refer to the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide* for more information.

## Anti-spam

Messaging Security Agent screens each email message for spam before delivery to the Exchange Information Store. The Exchange server will not process spam messages and these messages are not delivered to your user's mailboxes.

Administrators can set the **spam detection level** to screen out spam. The detection level determines how tolerant a Messaging Security Agent will be towards suspect email messages. A high detection level identifies and quarantines most spam, but it

might also falsely identify and quarantine legitimate email messages as spam, creating “false positive” spam mail. A low detection level does not rigorously screen email messages nor does it create many false positive spam messages.

Messaging Security Agent can screen spam according to seven categories and allows administrators to specify a detection level for each category. You customize your detection levels for Adult, Commercial, Financial, Spiritual, Health, Racial, or Others categories.

For example, if your users work in the banking industry, the administrator might decide to set a high sensitivity level for the “adult” category - messages in this category are very likely to be classified as spam. However, it might be more difficult to filter “commercial” type messages. Therefore, the administrator can set a low sensitivity level for email messages in the “commercial” category.

If you installed End User Quarantine, every end user protected by Messaging Security Agent has a special quarantine folder called “Spam Mail” in their mailbox. The spam folder is created on the server-side, but the end user can manage the contents of the folder by creating an Approved Sender list.

### Default Settings

- Anti-spam is enabled, so Messaging Security Agent screens email messages in real time
- The spam detection rate is set to medium
- Whenever Messaging Security Agent detects a spam email message, it quarantines the spam message to the intended recipient’s spam folder
- By default, Messaging Security Agent also detects phishing incidents and deletes email messages containing these threats

## Content Filtering

Content Filtering evaluates inbound and outbound messages on the basis of user-defined rules. Each rule contains a list of keywords and phrases. Content filtering evaluates the header and/or content of messages by comparing the messages with the list of keywords. When the content filter finds a word that matches a keyword it can take action to prevent the undesirable content from being delivered to Exchange Clients. The Messaging Security Agent can send notifications whenever it takes an action against undesirable content.

The content filter provides a means for the administrator to evaluate and control the delivery of email messages on the basis of the message text itself. It can be used to monitor inbound and outbound messages to check for the existence of harassing, offensive, or otherwise objectionable message content. The content filter also provides a synonym checking feature, which allows you to extend the reach of your policies. You can, for example, create rules to check for:

- Sexually offensive or explicit language
- Racist language
- Spam embedded in the body of an email message

### Default Settings

Content Filtering is disabled.

## Attachment Blocking

Attachment Blocking prevents Internet threats in email message attachments from being delivered to the Exchange Information Store. Configure Messaging Security Agent to block attachments according to the attachment type or attachment name. Then, configure Messaging Security Agent to *replace*, *quarantine*, or *delete the entire message.*

### Default Settings

Attachment Blocking is disabled by default. If enabled, MSA blocks the files with the following extensions. Files with these extensions are more likely to harbor viruses and other threats:

`ADE, ADP, ASX, BAS, BAT, BIN, CHM, CMD, COM, CPL, CRT, DLL, EML, EXE, HIV, HLP, HTA, INF, INS, ISP, JS, JSE, JTD, MSC, MSI, MSP, MST, OCX, OFT, OVL, PCD, PIF, PL, PLX, SCR, SCT, SH, SHB, SHS, SYS, VB, VBE, VBS, VSS, VST, VXD, WSC, WSF,` and `WSH`.

When Messaging Security Agent detects a threat in one of these specified files, it replaces the threat with a harmless text string or file that informs the intended recipient that the threat was detected and removed.

You can customize the attachments Messaging Security Agent blocks and the action that it performs on detected files. For more information, refer to the *Online Help*.

### Quarantine

When Messaging Security Agent quarantines an email message, the MSA logs an event and sends the email message to a designated quarantine folder. You can query the quarantine database to gather information about quarantined messages.

Messaging Security Agent quarantines email messages according to the actions you set. You can create one quarantine folder for each filter: Antivirus, Attachment Blocking, Anti-spam, and Content Filtering.

#### Default Settings

- **Antivirus Quarantine Directory.** `C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\`
- **Anti-spam Quarantine Directory.** `C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\`
- **Content Filtering Quarantine Directory.** `C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\`
- **Attachment Blocking Quarantine Directory.** `C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\`

### Operations

Perform spam maintenance, set internal email address, and set system debugger options.

## Configuring Reports

Configure Worry-Free Business Security Advanced to generate and send reports to administrators and managers periodically. Administrators can configure the content included in the report, the frequency, and the recipient list.

Generate One-time Reports to view log information in an organized and graphically appealing format. You can print reports or send them by email to an administrator or other specified recipients.

# Setting Global Preferences

Click **Preferences > Global Settings** to open the **Global Settings** screen and configure proxy server and SMTP server. You can also use it to configure System and Desktop/Server settings that apply to all the computers protected by Worry-Free Business Security Advanced.

Trend Micro provides default settings for global preferences. If you want to customize your settings, refer to the Trend Micro™ Worry-Free™ Business Security Advanced *Administrator's Guide* or the *Online Help*.

Chapter 8

# Technical Support

This chapter tells you how to solve common problems and how to contact technical support. This chapter includes the following topics:

# Contacting Trend Micro

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

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

**Note:** The information on this Web site is subject to change without notice.

# Trend Micro Support

Trend Micro Support can help you resolve queries relating to your Trend Micro products. Most queries have already been answered on the Knowledge Base (refer *Knowledge Base* on page 8-2 for more information). If you cannot find your answer on the Knowledge Base, you can contact Trend Micro Technical Support for further assistance (refer to *Contacting Technical Support* on page 8-2 for more information).

## 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 infections, and regional contact information for support and sales.

The Knowledge Base can be accessed by visiting:

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

## Contacting Technical Support

When you contact Trend Micro Technical Support, to speed up your problem resolution, run the Case Diagnostic Tool (refer to *Using the Case Diagnostic Tool* on page 8-3) 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 computer
- Detailed description of the installation environment
- Exact text of any error message
- Steps to reproduce the problem

**To contact Trend Micro Technical Support:**

1. Run the Case Diagnostic Tool. For more information, refer *Using the Case Diagnostic Tool* on page 8-3.
2. Visit the following URL:

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

3. Click the link for the required region. Follow the instructions for contacting support in your region.

### Using the Case Diagnostic Tool

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

Download the Case Diagnostic Tool from:

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

## About Trend Micro

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. Founded in 1988, Trend Micro led the migration of virus protection from the desktop to the network server and the Internet gateway, gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impact of threats to information by offering centrally controlled, server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and

file servers, Trend Micro enables companies and service providers worldwide to stop Internet threats from a central point, before they ever reach the desktop.

To make this possible, TrendLabs, a global network of antivirus research and product support centers, provides continuous 24 x 7 coverage to Trend Micro customers around the world. TrendLabs' modern headquarters has earned ISO 9002 certification for its quality management procedures—one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

Trend Micro is headquartered in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia—a global organization with more than 3,000 employees in 30 countries.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

**http://www.trendmicro.com**

Appendix A

# Best Practices to Protect Your Computers and Network

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 Worry-Free Business Security Advanced 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. Internet threats may be masked as other types of files your users may want to download, such as MP3 music files.
- Periodically examine the installed software on the computers on your network. If you find an application or file that Worry-Free Business Security Advanced 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.

  If you prefer to communicate using email, send 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 B

# Glossary of Terms

The following is a list of terms in this document:

| Term | Description |
|---|---|
| **ActiveUpdate** | Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of components such as the virus pattern files, scan engines, and program files.<br><br>ActiveUpdate is a function common to many Trend Micro products. |
| **ActiveUpdate Server** | The server that provides the ActiveUpdate functionality. |
| **ActiveX malicious code** | A type of virus that resides in Web pages that execute ActiveX controls. |
| **Administrator** | The person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security. |
| **Administrator account** | An account with administrator privileges. |
| **Anti-spam** | Refers to a filtering mechanism designed to identify and prevent delivery of unsolicited email messages. |
| **Attachment** | A file attached to (sent with) an email message. |
| **Body (message body)** | The content of an email message. |

| Term | Description |
|---|---|
| **Boot sector virus** | A sector is a designated portion of a disk (the physical device on which data is written and read). The boot sector contains the data used by your computer to load and initialize the computer's operating system. A boot sector virus infects the boot sector of a partition or a disk. |
| **Bot** | 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. |
| **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. |
| **Client** | A computer system or process that requests a service of another computer system or process (a “server”) using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture. Note that the online help uses the term “Client computer” in a special way to refer to computers that form a client-server relationship to the Worry-Free Business Security Advanced main program, the Security Server. |
| **Client Computer** | Client Computers are Exchange servers, desktops, portable computers, and servers where a Messaging Security Agent or a Client/Server Security Agent is installed. |
| **Compressed file** | A single file or multiple files that has/have been reduced in size by a compression software.<br><br>A single file containing one or more separate files that have been reduced in size by a compression software. User must decompress these files before they can be viewed or used. Example of compression software are WinZip and WinRar. |
| **COM and EXE file infectors** | A type of virus that masquerades as an application by using a .exe or .com file extension. |
| **Content Filtering** | Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography. |
| **Content violation** | An event that has triggered the content filtering policy. |
| **Denial of Service Attack (DoS Attack)** | An attack on a computer or network that causes a loss of 'service', namely a network connection. Typically, DoS attacks negatively affect network bandwidth or overload computer resources, such as memory. |
| **Domain name** | The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called “name resolution”, uses the Domain Name System (DNS). |

| Term | Description |
|---|---|
| **Dynamic Host Control Protocol (DHCP)** | A device, such as a computer or switch, must have an IP address to be connected to a network, but the address does not have to be static. A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network. |
| **Encryption** | Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. Lacing decryption codes, Client/Server Security Agents can not scan encrypted files.<br><br>Real-Time Scan will scan the encrypted file when a user decrypts the file. |
| **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.<br><br>Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software. |
| **Exception** | Exceptions, in relation to the Firewall, are a list of computers, ports, and communication protocols that will not be blocked by the Firewall. Exceptions also describe the ports that you have set so that they are never blocked during Outbreak Defense protection measures. |
| **False positive** | A false positive occurs when a threat, Web site, URL, “infected” file, or email message is incorrectly determined by filtering software to be of an unwanted type. |
| **File name extension** | The portion of a file name (such as .dll or .xml), which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run. |
| **File type** | The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file. |
| **Firewall** | Firewalls create a barrier between the Internet and your local network to protect the local network from hacker attacks and network viruses. Firewalls examine data packet to determine if they are infected with a network virus. |
| **FQDN (fully qualified domain name)** | A fully qualified domain name (FQDN) consists of a host and domain name, including top-level domain. For example, www.trendmicro.com is a fully qualified domain name: www is the host, trendmicro is the second-level domain, and .com is the top-level domain. |

| Term | Description |
|---|---|
| **FTP (file transfer protocol)** | FTP is a standard protocol used for transporting files from a server to a client. |
| **Grayware** | Files and programs, other than viruses, that can negatively affect the performance of the computers on your network. These include spyware, adware, dialers, joke programs, hacking tools, remote access tools, password cracking applications, and others. The Worry-Free Business Security Advanced scan engine scans for grayware as well as viruses. |
| **Hot fix and patch** | Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the Worry-Free Business Security Advanced server and/or client program. |
| **Hyper Text Transfer Protocol (HTTP)** | HTTP is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet. |
| **HTTPS** | Hypertext Transfer Protocol using Secure Socket Layer (SSL). |
| **IntelliScan** | IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name. |
| **Internet Protocol (IP)** | Internet Protocol is a standardized method of transporting information across the Internet in packets of data. It is often linked to Transmission Control Protocol, which assembles the packets once they have been delivered to the intended location. |
| **Internet Threat** | An umbrella term to describe viruses, Trojans, DoS, spyware, spam, adware, joke programs, mixed threats, network viruses, phish, and so on.<br>Internet threats, depending on their type, may or may not include replicating and non replicating malicious code. |
| **(IDS)** | Intrusion Detection Systems are commonly part of firewalls. An IDS can help identify patterns in network packets that may indicate an attack on a Client. |
| **Keywords** | Messaging Security Agent can filter incoming email messages for keywords that you set up using Content Filtering rules. When keywords are detected, Messaging Security Agent can take action to prevent the delivery of messages containing these keywords. Note that keywords are not strictly words, but can be numbers, special characters, or short phrases. |
| **Local** | The term “local” refers to a computer on which you are directly installing or running software, as opposed to a “remote” computer which is physically distant and/or connected to your computer through a network. |
| **Macro virus** | A type of virus encoded in an application macro and often included in a document. |

| Term | Description |
|---|---|
| **Message body** | The content of an email message. |
| **Network virus** | Viruses that use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of computers, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. |
| **Notification** | The Security Server can send your system administrator a notification whenever significant abnormal events occur on your Client computers. For example, you can set up a condition that whenever Client/Server Security Agent detects 40 viruses within one hour, the Security Server will send a notification to the system administrator. |
| **Outbreak Defense** | During Outbreak Defense, the Security Server enacts the instructions contained in the Outbreak Prevention Policy. A Trend Micro Outbreak Prevention Policy is a set of recommended default security configuration and settings designed by TrendLabs to give optimal protection to your computers and network during outbreak conditions. The Security Server downloads an Outbreak Prevention Policy from Trend Micro ActiveUpdate Server every 30 minutes or whenever the Security Server starts up. Outbreak Defense enacts preemptive measures such as blocking shared folders, blocking ports, updating components, and running scans. |
| **Phishing incident** | A Phishing incident starts with an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click a link that will redirect their browsers to a fraudulent Web site. Here the user is asked to update personal information such as passwords, social security numbers, and credit card numbers in an attempt to trick a recipient into providing private information that may be used for identity theft. |
| **Phishing site** | A Web site that lures users into providing personal details, such as credit card information. Links to phishing sites are often sent in bogus email messages disguised as legitimate messages from well-known businesses. |
| **Ping of Death** | A Denial of Service attack where a hacker directs an oversized ICMP packet at a target computer. This can cause the computers buffer to overflow, which can freeze or reboot the computer. |
| **Post Office Protocol 3 (POP3)** | POP3 is a standard protocol for storing and transporting email messages from a server to a client email application. |
| **Port number** | A port number, together with a network address - such as an IP number, allow computers to communicate across a network. Each application program has a unique port number associated with it. Blocking a port on a computer prevents an application associated with that port number from sending or receiving communications to other applications on other computers across a network. Blocking the ports on a computer is an effective way to prevent malicious software from attacking that computer. |

| Term | Description |
|---|---|
| **Privileges (desktop privileges)** | From the Web console, administrators can set privileges for Client/Server Security Agents. End users can then configure Client/Server Security Agents to scan their computers according to the privileges you allowed. Use desktop privileges to enforce a uniform antivirus policy throughout your organization. |
| **Proxy server** | A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. |
| **Quarantine** | To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server. |
| **Remote** | The term “remote” refers to a computer that is connected through a network to another computer, but physically distant from that computer. |
| **Rule, content filtering** | Content filtering rules are rules that you set up to filter the content of email messages. You define undesirable content and sources and set Messaging Security Agent to detect and take action against such content violations. |
| **Scan** | To examine items in a file in sequence to find those that meet a particular criteria. |
| **Scan engine** | The module that performs antivirus scanning and detection in the host product on which it is integrated. |
| **Secure Socket Layer (SSL)** | SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a public-and-private key encryption system, which also includes the use of a digital certificate. |
| **SSL certificate** | A digital certificate that authenticates network entities such as a server or a client. |
| **Web console** | The Web console is a centralized Web-based management console. You can use it to configure the settings of Client/Server Security Agents and Messaging Security Agents, which are protecting all your Exchange servers, desktops, and servers. The Web console is installed when you install the Trend Micro Security Server and uses Internet technologies such as ActiveX, CGI, HTML, and HTTP. |
| **Security Server** | When you first install Worry-Free Business Security Advanced, you install it on a Windows server that becomes the Security Server. The Security Server communicates with Client/Server Security Agents and Messaging Security Agents installed on Client computers. The Security Server also hosts the Web console, the centralized Web-based management console for the entire Worry-Free Business Security Advanced solution. |

| Term | Description |
|---|---|
| **Server** | A program, which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the Client's requests and the server's responses. Note that the online help uses the term “Security Server” in a special way to refer to the server that forms a client-server relationship with the computers on your network on which you installed Client/Server Security Agents. |
| **Simple Mail Transport Protocol (SMTP)** | SMTP is a standard protocol used to transport email messages from server to server, and client to server. |
| **SOCKS 4** | A TCP protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model. |
| **Spam** | Unsolicited email messages meant to promote a product or service. |
| **Telnet** | Telnet is a standard method of interfacing terminal devices over TCP by creating a “Network Virtual Terminal”. |
| **Test virus** | An inert file that acts like a real virus and is detectable by virus-scanning software. Use test files, such as the EICAR test script, to verify that your antivirus installation is scanning properly. |
| **Transmission Control Protocol (TCP)** | A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols, which support multi-network applications. TCP relies on IP datagrams for address resolution. |
| **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. |
| **Trojan horse** | A Trojan horse is a malicious program that is disguised as legitimate software. The term is derived from the classical myth of the Trojan horse. |
| **Update** | Updating describe a process of downloading the most up-to-date components such as pattern files and scan engines to your computer. |
| **Virus** | A virus is a program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes. |
| **Vulnerability** | 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. |
| **Wildcard** | Wildcard actually refers to the asterisk (or any symbol) used to represent one or more characters. For example, in the expression `*ber`, this expression can represent `barber, number, plumber, timber`, and so on. |

| Term | Description |
|---|---|
| **Worm** | A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often through email. |

# Index

## R



## S



## T

## U



## V



## W