



Worry-Free™ Business Security Standard and Advanced Editions

#1 at stopping threats before they reach your business

Administration Guide

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

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

Trend Micro, the Trend Micro t-ball logo, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan, and ScanMail are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2010. Trend Micro Incorporated. All rights reserved.

Document Part Number: WBEM74598/100819

Release Date: October 2010

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

Document Version No.: 1.01

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

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

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

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

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

Contents

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

Overview of Trend Micro Worry-Free Business Security	1-2
What's New	1-2
Version 7.0	1-2
Key Features	1-3
The Trend Micro Smart Protection Network	1-3
Smart Feedback	1-3
Web Reputation	1-4
Email Reputation (Advanced only)	1-4
File Reputation	1-4
Smart Scan	1-5
URL Filtering	1-5
Benefits of Protection	1-5
Defense Components	1-6
Understanding Threats	1-10
Network Components	1-15
Sending Trend Micro Your Viruses	1-16

Chapter 2: Getting Started

Registering	2-2
Introducing the Web Console	2-2
Live Status	2-7
Viewing Computers	2-11

Key Components	2-13
Security Server	2-13
Security Agent	2-13
Web Console	2-14
Clients	2-14
Virus Scan Engine	2-14

Chapter 3: Installing Agents

Security Agent Installation/Upgrade/Migration Overview	3-2
Installing Security Agents to Desktops and Servers	3-2
Performing a Fresh Install	3-5
Installing from an Internal Web Page	3-5
Installing with Login Script Setup	3-6
Installing with Client Packager	3-9
Installing with an MSI File	3-11
Installing with Remote Install	3-12
Installing with Vulnerability Scanner	3-14
Installing with Email Notification	3-16
Installing MSA from the Web Console (Advanced only)	3-16
Verifying the Agent Installation, Upgrade, or Migration	3-17
Verifying Client Installation with Vulnerability Scanner	3-18
Verifying Client-Server Connectivity	3-19
Testing the Client Installation with the EICAR Test Script	3-20
Removing Agents	3-20
Removing the SA Using the Agent Uninstallation Program	3-21
Removing the SA Using the Web Console	3-21
Removing the Agent from Exchange Servers (Advanced only)	3-22
Running the Messaging Security Agent Uninstallation Program (Advanced only)	3-22

Chapter 4: Managing Groups

Groups	4-2
Adding Groups	4-4
Adding Clients to Groups	4-5
Moving Clients	4-5
Replicating Group Settings	4-6
Importing and Exporting Settings	4-6
Removing Computers from the Web Console	4-7
Removing Inactive Security Agents	4-8

Chapter 5: Managing Basic Security Settings

Options for Desktop and Server Groups	5-2
Configuring Real-time Scan	5-4
Managing the Firewall	5-4
Configuring the Firewall	5-7
Working with Firewall Exceptions	5-9
Disabling the Firewall	5-11
Intrusion Detection System	5-11
Web Reputation	5-13
Configuring Web Reputation	5-14
URL Filtering	5-16
Behavior Monitoring	5-17
Device Control	5-20
User Tools	5-22
Configuring User Tools	5-22
Configuring Client Privileges	5-23
Configuring the Quarantine	5-25
Configuring the Quarantine Directory	5-26

Chapter 6: Managing Scans

About Scanning	6-2
Scan Types	6-2
Scan Methods	6-3
Selecting the Scan Method	6-4
Enabling Real-Time Scanning	6-4
Running Manual Scans on Desktops and Servers	6-5
Virus Pattern	6-6
Running Scheduled Scans for Desktops and Servers	6-7
Scheduling Scans	6-9
Configuring Antivirus/Anti-Spyware Scans for Desktops and Servers	6-10
Modifying the Spyware/Grayware Approved List	6-14
Uncleanable Files	6-16
Mail Scan	6-17
Trojan Ports	6-18

Chapter 7: Managing Updates

Updating the Security Server	7-2
Hot Fixes, Patches, and Service Packs	7-3
Updating Security Agents	7-3
ActiveUpdate	7-4
Agent Update Sources	7-5
Configuring an Update Source for the SS and Agents	7-5
Configuring Alternative Update Sources for Security Agents	7-8
Update Agents	7-10
Using Update Agents	7-13
Manually Updating Components	7-15
Scheduling Component Updates	7-16
Updatable Components	7-18

Chapter 8: Managing Notifications

Notifications	8-2
Configuring Events for Notifications	8-3
Customizing Notification Email Messages	8-6
Tokens	8-6
Configuring Notification Settings for Microsoft Exchange Servers (Advanced only)	8-7

Chapter 9: Managing the Messaging Security Agent (Advanced only)

Messaging Security Agents	9-3
Messaging Security Agent Actions	9-5
Configuring Scan Options for Microsoft Exchange Servers	9-7
Installing MSAs to Microsoft Exchange Servers	9-9
Removing Microsoft Exchange Servers from the Web Console	9-11
Antivirus	9-12
Configuring Real-Time Scans for Exchange Servers	9-13
Manual Scans for Microsoft Exchange Servers	9-17
Scheduled Scans for Microsoft Exchange Servers	9-19
Configuring Manual or Scheduled Scans for Exchange Servers	9-20
Anti-Spam	9-23
Configuring Anti-Spam	9-24
Spam Detection Settings	9-25
Managing End User Quarantine	9-26
Email Reputation	9-28
Content Scanning	9-30
Phishing Incidents	9-32
Detecting and Removing Phishing Incidents	9-32
Content Filtering	9-39
Adding/Editing Content Filtering Rules	9-41
Creating Content Filtering Rules	9-43
Creating Content Filtering Rules for All Matching Conditions	9-45
Creating Exceptions to Content Filtering Rules	9-46

Editing Content Filtering Rules	9-47
Removing Content Filtering Rules	9-49
Data Loss Prevention	9-65
Preparatory Work	9-66
Data Loss Prevention Rules	9-66
Pre-approved Domains and Approved Senders	9-82
Attachment Blocking	9-87
Selecting Blocking Targets	9-87
Attachment Blocking Actions	9-88
Configuring Attachment Blocking	9-89
Real-time Monitor	9-90
Web Reputation	9-91
Configuring Web Reputation Settings	9-93
Messaging Agent Quarantine	9-93
Configuring Quarantine Directories	9-94
Agent Quarantine Folder	9-96
Querying Quarantine Directories	9-97
Maintaining Quarantine Directories	9-100
Managing the End User Quarantine Tool	9-101
Operations	9-102
Notification Settings	9-103
Spam Maintenance	9-105
Trend Support/Debugger	9-106
Replicating Settings for Microsoft Exchange Servers	9-108
Adding a Disclaimer to Outbound Email Messages	9-108
Configuring Exclusions for Messaging Security Agents	9-109
Advanced Scan Options for Microsoft Exchange Servers	9-111
Advanced Macro Scanning	9-112
Internal Address Definition	9-113

Chapter 10: Using Outbreak Defense

Outbreak Defense Strategy	10-2
Outbreak Defense Current Status	10-4
Threat Cleanup	10-6
Vulnerability Assessment	10-7
Vulnerability Assessment Pattern File	10-7
Potential Threat	10-8
Configuring Outbreak Defense Settings	10-10
Outbreak Defense Exceptions	10-14
Removing Ports from the Exceptions List	10-16
Configuring Vulnerability Assessment Settings	10-16
Cleanup Services	10-17
Viewing Automatic Outbreak Defense Details	10-18

Chapter 11: Managing Global Settings

Configuring Global Preferences	11-2
Internet Proxy Options	11-3
SMTP Server Options	11-5
Desktop/Server Options	11-6
System Options	11-13

Chapter 12: Using Logs and Reports

Logs	12-2
Using Log Query	12-4
Deleting Logs	12-6
Reports	12-7
One-Time Reports	12-8
Interpreting Reports	12-8
Generating Reports	12-11
Adding a Scheduled Report	12-12
Editing Scheduled Reports	12-13

Managing Logs and Reports	12-14
Maintaining Reports	12-14
Viewing Report History	12-15

Chapter 13: Administering WFBS

Changing the Web Console Password	13-2
Working with the Plug-in Manager	13-3
Viewing Product License Details	13-3
Participating in the Smart Protection Network	13-5
Changing the Agent's Interface Language	13-6
Uninstalling the Trend Micro Security Server	13-6

Appendix A: Client Information

Client Icons	A-2
Agent Tray Icons	A-3
Agent FlyOver Icons	A-4
Agent Main Console Icons	A-6
Location Awareness	A-8
32-bit and 64-bit Clients	A-8

Appendix B: Using Management (Administrative and Client) Tools

Tool Types	B-2
Administrative Tools	B-3
Login Script Setup	B-3
Vulnerability Scanner	B-3
Using the Vulnerability Scanner	B-4
About the Worry-Free Remote Manager Agent	B-7
Free Disk Space	B-9
Disk Cleaner Tool	B-9

Client Tools	B-11
Client Packager	B-11
Restoring an Encrypted Virus	B-12
Client Mover Tool	B-14
Add-ins	B-16
SBS and EBS Add-ins	B-17

Appendix C: Troubleshooting and Frequently Asked Questions

Troubleshooting	C-2
Unable to Replicate Messaging Security Agent Settings (Advanced only)	
C-10	
Frequently Asked Questions (FAQs)	C-11
Where Can I Find My Activation Code and Registration Key?	C-11
Registration	C-12
Installation, Upgrade, and Compatibility	C-12
How Can I Recover a Lost or Forgotten Password?	C-13
Intuit Software Protection	C-13
Configuring Settings	C-13
Do I Have the Latest Pattern File or Service Pack?	C-15
Smart Scan	C-16
Known Issues	C-17

Appendix D: Trend Micro Services

Outbreak Prevention Policy	D-2
Damage Cleanup Services	D-2
Vulnerability Assessment	D-3
IntelliScan	D-4
ActiveAction	D-4
IntelliTrap	D-6

Email Reputation Services (Advanced only)	D-7
Web Reputation	D-8

Appendix E: Trend Micro Security for Mac Plug-in

About Trend Micro Security for Mac	E-2
The Trend Micro Security Client	E-3
Installing the Trend Micro Security Server for MAC	E-4
Server Installation Requirements	E-4
Operating System Requirements	E-5
Hardware Requirements	E-8
Update Source	E-9
Server Installation	E-9
Server Post-Installation	E-13
Server Uninstallation	E-15
Getting Started with Trend Micro Security	E-15
The Web Console	E-15
Security Summary	E-16
The Trend Micro Security Client Tree	E-17
Trend Micro Security Groups	E-20
Installing the Trend Micro Security Client	E-21
Client Installation Requirements	E-21
Client Installation Methods	E-22
Client Postinstallation	E-29
Client Uninstallation	E-31
Keeping Protection Up-to-Date	E-32
Components	E-32
Update Overview	E-33
Server Update	E-34
Client Update	E-37

Protecting Computers from Security Risks E-38

 About Security Risks E-38

 Scan Types E-42

 Settings Common to All Scan Types E-45

 Security Risk Notifications E-51

 Security Risk Logs E-54

 About Web Threats E-57

 Web Reputation E-57

 Web Reputation Policies E-57

 Approved URLs E-58

 Web Reputation Logs E-59

Managing the Trend Micro Security Server and Clients E-60

 Upgrading the Server and Clients E-60

 Managing Logs E-63

 Licenses E-64

 Client-Server Communication E-65

 Mac Client Icons E-67

Troubleshooting and Support E-69

 Troubleshooting E-69

 Security Information Center E-73

**Appendix F: TSM Installation and Configuration
Worksheet**

Server Installation F-2

Client Installation F-5

Server Configuration F-7

**Appendix G: Migrating from Other Anti-Malware
Applications**

Migrating from Other Anti-Malware Applications G-2

Appendix H: Best Practices for Protecting Your Clients

Best Practices H-2

Appendix I: Getting Help

Product Documentation I-2

Knowledge Base I-3

Technical Support I-3

Contacting Trend Micro I-4

 Sending Suspicious Files to Trend Micro I-5

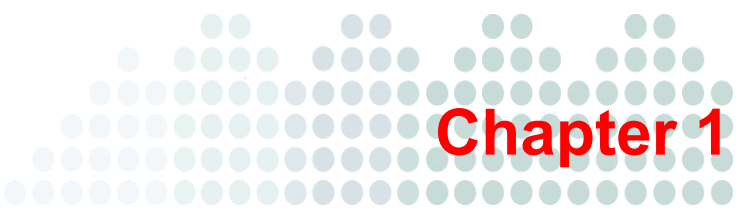
Virus Threat Encyclopedia I-6

 TrendLabs I-7

Appendix J: Glossary

Appendix K: Trend Micro Product Exclusion List

Exclusion List for Microsoft Exchange Servers (Advanced only) K-5



Chapter 1

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

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

The topics discussed in this chapter include:

- *Overview of Trend Micro Worry-Free Business Security* on page 1-2
- *What's New* on page 1-2
- *Key Features* on page 1-3
- *Benefits of Protection* on page 1-5
- *Defense Components* on page 1-6
- *Understanding Threats* on page 1-10
- *Network Components* on page 1-15
- *Sending Trend Micro Your Viruses* on page 1-16

Overview of Trend Micro Worry-Free Business Security

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

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

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

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

What's New

Version 7.0

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

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

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

Key Features

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

The Trend Micro Smart Protection Network



Protection Network.

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

Smart Feedback

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

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

Web Reputation

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

Email Reputation (Advanced only)

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

File Reputation

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

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

Smart Scan

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

URL Filtering

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

Benefits of Protection

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

TABLE 1-1. Benefits of Protection

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

TABLE 1-1. Benefits of Protection (Continued)

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

Defense Components

Antivirus/Anti-spyware

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

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

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

Anti-spam

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

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

Outbreak Defense

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

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

Network Virus

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

Web Reputation

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

Trend Micro Toolbar

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

Software Protection

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

Behavior Monitoring

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

Wi-Fi Advisor

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

Content Filtering

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

Live Status and Notifications

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

Understanding Threats

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

Virus/Malware

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

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

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

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

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

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

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

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

Spyware/Grayware

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

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

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

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

Network Viruses

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

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

Spam

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

Intrusions

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

Malicious Behavior

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

Fake Access Points

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

Explicit/Restricted Content in IM Applications

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

Online Keystroke Listeners

An online version of a keylogger. See [Spyware/Grayware](#) on page 1-11 for more information.

Packers

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

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

Phishing Incidents (Advanced only)

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

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

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

Mass-Mailing Attacks (Advanced only)

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

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

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

Network Components

Worry-Free Business Security uses the following components:

TABLE 1-2. Network Components

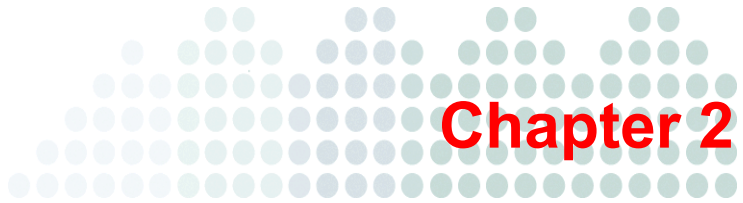
CONVENTION/TERM	DESCRIPTION
Security Server	The Security Server hosts the Web Console, the centralized Web-based management console for the entire Trend Micro™ Worry-Free™ Business Security solution.
Web Console	The Web Console is a centralized, management console that manages all the Agents. The Web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

Sending Trend Micro Your Viruses

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

<http://subwiz.trendmicro.com/subwiz>

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



Getting Started

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

Registering on page 2-2

Introducing the Web Console on page 2-2

Live Status on page 2-7

Viewing Computers on page 2-11

Key Components on page 2-13

Registering

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

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

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

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

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

<http://olr.trendmicro.com>

Introducing the Web Console

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

Use the following menu options from Web Console:

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

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

The console contains the following, main sections:

TABLE 2-1. Web Console Main Features

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

To open the Web Console:

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

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

For example:

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

`https://192.168.0.10:4343/SMB`

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

http://192.168.0.10:8059/SMB

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

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

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

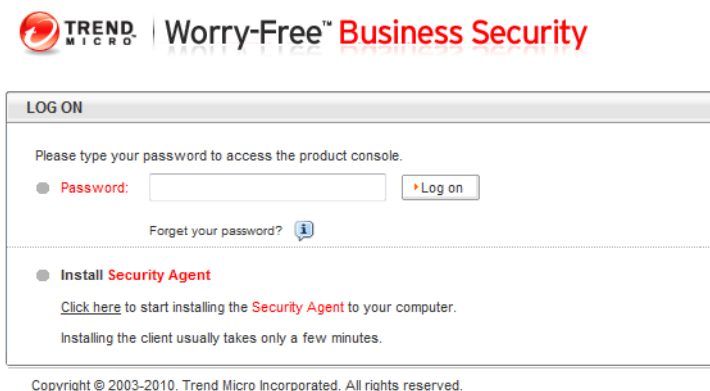


FIGURE 2-1. Logon screen of WFBS

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

Web Console Icons

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

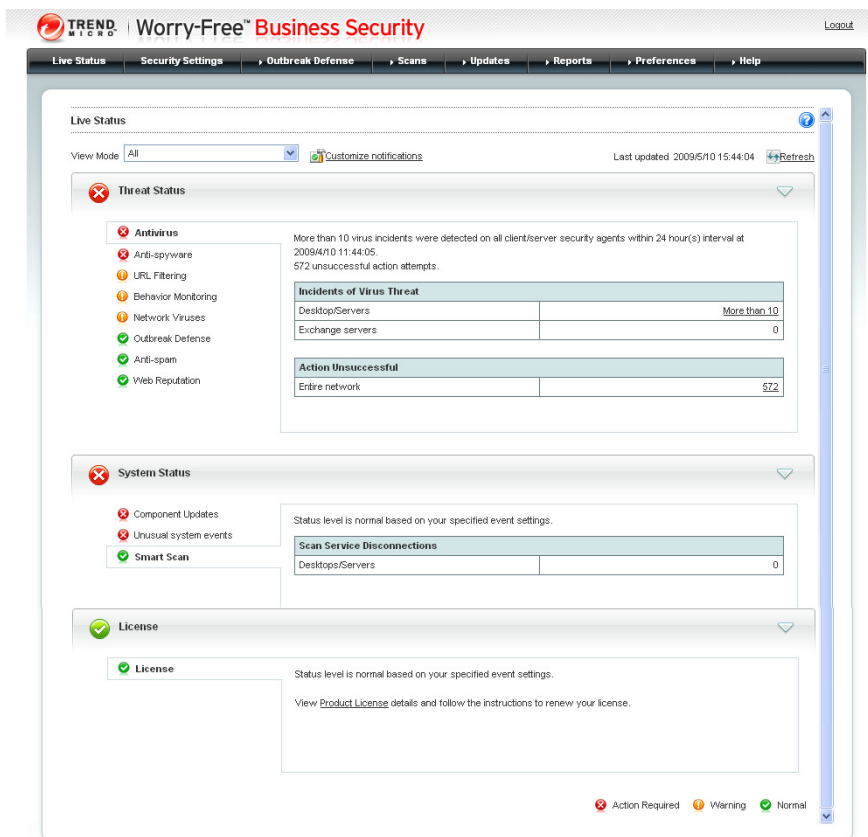
TABLE 2-2. Web Console Icons

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

Live Status

Use the Live Status screen to manage WFBS.

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



TREND MICRO Worry-Free Business Security Logout

Live Status Security Settings Outbreak Defense Scans Updates Reports Preferences Help

Live Status View Mode: All Customize notifications Last updated: 2009/5/10 15:44:04 Refresh

Threat Status

Antivirus

- Anti-spyware
- URL Filtering
- Behavior Monitoring
- Network Viruses
- Outbreak Defense
- Anti-spam
- Web Reputation

More than 10 virus incidents were detected on all client/server security agents within 24 hour(s) interval at 2009/5/10 11:44:05.
572 unsuccessful action attempts.

Incidents of Virus Threat	
Desktop/Servers	More than 10
Exchange servers	0

Action Unsuccessful	
Entire network	572

System Status

- Component Updates
- Unusual system events
- Smart Scan

Status level is normal based on your specified event settings.

Scan Service Disconnections	
Desktops/Servers	0

License

- License

Status level is normal based on your specified event settings.
View [Product License](#) details and follow the instructions to renew your license.

⛔ Action Required
⚠ Warning
✅ Normal

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

Understanding Icons

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

TABLE 2-3. Live Status Icons

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

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

Threat Status

Displays information about the following:

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

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

System Status

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

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

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

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

License Status

Information regarding the license status.

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

Live Status Update Intervals

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

TABLE 2-4. Live Status Update Intervals

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

TABLE 2-4. Live Status Update Intervals (Continued)

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

Viewing Computers

Navigation Path: Security Settings {tab}

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

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

Global Navigation Menu

These menu items are always available.

Configuration Area

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

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

Toolbar:

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

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

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

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

Key Components

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

Security Server

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

The Security Server performs these important functions:

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

Security Agent

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

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

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

Web Console

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

Also use the Web Console to:

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

Control outbreaks by configuring and enabling Outbreak Prevention.

Clients

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

Virus Scan Engine

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

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

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

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

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

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

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

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

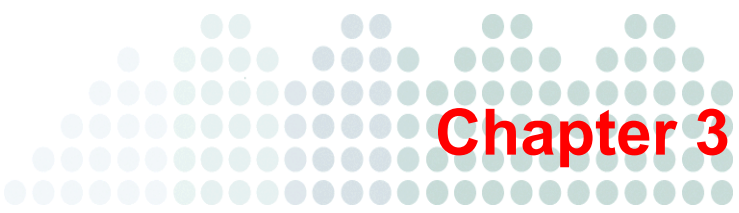
Scan Engine Updates

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

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

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

<http://www.trendmicro.com>



Chapter 3

Installing Agents

This chapter explains the steps necessary for installing or upgrading the Trend Micro Worry-Free Business Security Agent. It also provides information on removing Security Agents.

The topics discussed in this chapter include:

- *Security Agent Installation/Upgrade/Migration Overview* on page 3-2
- *Installing Security Agents to Desktops and Servers* on page 3-2
- *Performing a Fresh Install* on page 3-5
- *Verifying the Agent Installation, Upgrade, or Migration* on page 3-17
- *Removing Agents* on page 3-20

Security Agent Installation/Upgrade/Migration Overview

This section provides information on the following:

- Performing a fresh Security Agent install with your chosen installation method (see [Performing a Fresh Install](#) on page 3-5)
- Upgrading from a previous version of Security Agent to the current version (see [Verifying the Agent Installation, Upgrade, or Migration](#) on page 3-17)
- Migrating from a third-party antivirus installation to the current version of WFBS (see [Verifying the Agent Installation, Upgrade, or Migration](#) on page 3-17)

Note: Close any running applications on clients before installing the Security Agent. If you install while other applications are running, the installation process may take longer to complete.

Installing Security Agents to Desktops and Servers

Navigation Path: Security Server > Add

Immediately following the installation, Worry-Free Business Security adds icons for the Clients to the Security Settings screen and notifies those Clients to install the Security Agent.

- If you have installed Worry-Free Business Security for the first time, you will see two default computer groups in this screen: Servers and Clients. Worry-Free Business Security automatically adds the computers and servers it detects on your network to these groups.

- If you have upgraded Worry-Free Business Security from a previous or evaluation version, Worry-Free Business Security preserves your old computers and groups in the Security Groups Tree.

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

After installation, if you want to install the Security Agent to other desktops and servers, you must use the Web Console or another tool that was installed with Worry-Free Business Security.

- Use the **Security Settings** screen. Click **Add** and use one of the following methods:
 - **Email notification install:** Select this to send an email message with a link to the Security Agent installation program. *Installing with Email Notification* on page 3-16.
 - **Remote Install:** Select this to deploy the Security Agent remotely from the Security Server. See *Installing with Remote Install* on page 3-12.
 - **Login Script Setup:** Automate the installation of the Security Agent to unprotected computers when they log on to the domain. See *Installing with Login Script Setup* on page 3-6.
- Other methods using tools installed with Worry-Free Business Security:
 - **Internal Web page:** Instruct users in your organization to go to the internal Web page and download the Security Agent setup files. See *Installing from an Internal Web Page* on page 3-5.
 - **Client Packager:** Deploy the Security Agent setup or update files to Clients via email, CD-ROM, or similar media. See *Installing with Client Packager* on page 3-9.

- **Vulnerability Scanner (TMVS):** Install the Security Agent with the Trend Micro Vulnerability Scanner. See *Installing with Vulnerability Scanner* on page 3-14.

Tip: Trend Micro recommends Remote Install or Login Script Setup for organizations enforcing strict policies.

Note: To use any of these Security Agent deployment methods, you must have local Administrator rights on the target clients.

TABLE 3-1. Agent Deployment Methods

	WEB PAGE	LOGIN SCRIPTS	CLIENT PACKAGE R	REMOTE INSTALL	TMVS
Suitable for deployment across the WAN	Yes	No	Yes	No	No
Suitable for centralized administration and management	Yes	Yes	No	Yes	Yes
Requires user intervention	Yes	No	Yes	No	No
Requires IT resource	No	Yes	Yes	Yes	Yes
Suitable for mass deployment	No	Yes	No	Yes	Yes

TABLE 3-1. Agent Deployment Methods (Continued)

	WEB PAGE	LOGIN SCRIPTS	CLIENT PACKAGE R	REMOTE INSTALL	TMVS
Bandwidth consumption	Low, if schedule d	High, if clients are started at the same time	Low, if schedule d	Low, if scheduled	Low, if schedule d
Required Privileges	Administrator privileges required for all installation methods.				

Performing a Fresh Install

Follow one of the procedures below if this is the first time you are installing a Security Agent on target computers.

Installing from an Internal Web Page

If you installed the Trend Micro Security Server to a computer running Windows XP/Vista/7/Server 2003/Server 2008 with Internet Information Server (IIS) 5.0, 6.0, or 7.0 or Apache™ 2.0.63, users can install the Security Agent from the internal website created during master setup.

This is a convenient way to deploy the Security Agent. You only have to instruct users to go to the internal Web page and download the Security Agent setup files.

Tip: You can use Vulnerability Scanner to see which users have not followed the instructions to install from the Web Console (see *Verifying Client Installation with Vulnerability Scanner* on page 3-18 for more information).

Users must have Microsoft Internet Explorer™ 6.0 or later with the security level set to allow ActiveX controls to successfully download the Security Agent setup files. The instructions below are written from the user perspective. Email your users the following instructions to install the Security Agent from the internal Web server.

To install from the internal Web page:

1. Open an Internet Explorer window and type:

```
https://{Trend Micro Security  
Server_name}:{port}/SMB/console/html/client
```

For example:

```
https://my-test-server:4343/SMB/console/html/client  
http://my-test-server:8059/SMB/console/html/client  
https://192.168.0.10:4343/SMB/console/html/client  
http://192.168.0.10:8059/SMB/console/html/client
```

Or use the Web Console's URL. On the password screen, you will see a **Click here** link for client installation.

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

2. Click **Install Now** to start installing the Security Agent.

Note: For Windows Vista, ensure **Protected Mode** is enabled.
To enable **Protected Mode**, in Internet Explorer, click **Tools > Internet Options > Security**.

The installation starts. Once installation is completed, the screen displays the message, **Agent installation is complete**.

3. Verify the installation by checking if the Security Agent icon  appears in the Windows system tray.

Installing with Login Script Setup

Use Login Script Setup to automate the installation of the Security Agent on unprotected computers when they log on to the domain. Login Script Setup adds a program called `autopcc.exe` to the server login script. The program `autopcc.exe` performs the following functions:

- Determines the operating system of the unprotected computer and the Security Agent
- Updates the scan engine, virus pattern file, Damage Cleanup Services components, cleanup file, and program files

Note: In order to enforce the use of login script installation method, clients must be listed in the Windows Active Directory of the server that is performing the installation.

If you already have an existing login script for Windows Server 2003/Server 2008, Login Script Setup will append a command that executes `autopcc.exe`; otherwise, it creates a batch file called `ofcscan.bat` (contains the command to run `autopcc.exe`).

Login Script Setup appends the following at the end of the script:

```
\\{Server_name}\ofcscan
```

where:

{Server_name} is the computer name or IP address of the computer where the Trend Micro Security Server is installed.

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

The Server 2003 login script is on the Server 2003 server (through a net logon shared directory), under:

```
\\Windows 2003 server\{system drive}\%windir%\sysvol\
domain\scripts\ofcscan.bat
```

The Server 2008 login script is on the Server 2008 server (through a net logon shared directory), under:

```
\\Windows 2008 server\{system drive}\%windir%\sysvol\
domain\scripts\ofcscan.bat
```

To add autopcc.exe to the login script using Login Script Setup:

1. On the computer where you installed WFBS, open C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\SetupUsr.exe. The **Login Script Setup** utility loads. The console displays a tree showing all domains on your network.
2. Browse for the Windows Server 2003/Server 2008 computer whose login script you want to modify, select it, and then click **Select**. The server must be a primary domain controller and you must have Administrator access.
Login Script Setup prompts you for a user name and password.
3. Type your user name and password. Click **OK** to continue.
The **User Selection** screen appears. The **Users** list shows the computers that log on to the server. The **Selected users** list shows the users whose computer login script you want to modify.
 - To modify the login script of a single user or multiple users, select them from **Users** and then click **Add**
 - To modify the login script of all users, click **Add All**
 - To exclude a user whose computer you previously modified, select the name in **Selected users** and click **Delete**
 - To reset your choices, click **Delete All**
4. Click **Apply** when all the target users are in the **Selected users** list.
A message appears informing you that you have modified the server login scripts successfully.
5. Click **OK**. The Login Script Setup utility will return to its initial screen.
 - To modify the login scripts of other servers, repeat steps 2 to 4
 - To close Login Script Setup, click **Exit**

Note: When an unprotected computer logs on to the servers whose login scripts you modified, `autopcc.exe` will automatically install the Agent to it.

Installing with Client Packager

Client Packager can compress setup and update files into a self-extracting file to simplify delivery through email, CD-ROM, or similar media.

When users receive the package, all they have to do is double-click the file to run the setup program. Agents installed using Client Packager report to the server where Client Packager created the setup package. This tool is especially useful when deploying the Agent or update files to clients in low-bandwidth remote offices.

Client Packager Installation Considerations

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

Note: Client Packager requires a minimum of 370MB free disk space on the Client. Windows Installer 3.0 is necessary for the client to run an MSI package.

The Microsoft Installer Package Format (MSI) conforms to the Microsoft Windows Installer package specifications and can be used for silent and/or Active Directory deployment. For more information on MSI, see the Microsoft website.

Tip: Trend Micro recommends using Active Directory to deploy an MSI package with **Computer Configuration** instead of **User Configuration**. This helps ensure that the MSI package will be installed regardless of which user logs on to the machine.

To create a package with the Client Packager GUI:

1. On the Trend Micro Security Server, open Windows Explorer.
2. Go to \PCCSRV\Admin\Utility\ClientPackager.
3. Double-click ClnPack.exe to run the tool. The **Client Packager** console opens.

Note: You must run the program from the Trend Micro Security Server only.

4. Select the type of package you want to create:
 - **Setup:** Select if installing the Agent.
 - **Update:** Select if updating Security Agent components only.
5. In **Target operating system**, select the operating system for which you want to create the package.
6. Select the **Scan Method**.
 - **Conventional Scan:** a local scan engine on the client scans the client computer.
 - **Smart Scan:** a Scan Server helps scan the client. A Scan Server is automatically installed with the Security Server. You can choose the scan method on the Security Settings screen. Scan modes use different pattern files. Conventional Scan uses the traditional virus pattern file.
7. Select from among the following installation options under **Options**:
 - **Silent Mode:** Creates a package that installs on the client in the background, unnoticeable to the user. The installation status window will not appear.
 - **MSI Package:** Creates a package that conforms to the Microsoft Windows Installer Package Format.

Note: The MSI package is for Active Directory deployment only. For local installation, create an .exe package.

- **Disable Prescan (only for fresh-install):** Disables the normal file scanning that WFBS performs before starting setup.
8. Under **Components**, select the components to include in the installation package:
 - **Pack all:** Choose all components
 - **AntiVirus and Anti-spyware**
 - **Behavior Monitoring and Device Control**
 - **Network Virus**
 - **Outbreak Defense**
 - **Web Reputation**

9. Ensure that the location of the `ofcscan.ini` file is correct next to **Source file**. To modify the path, click  to browse for the `ofcscan.ini` file. By default, this file is located in the `\PCCSRV` folder of the Trend Micro Security Server.
10. In **Output file**, click  to specify the file name and the location to create the package.
11. Click **Create** to build the package. When Client Packager finishes creating the package, the message **Package created successfully** appears. To verify successful package creation, check the output directory you specified.
12. Send the package to your users through email, or copy it to a CD or similar media and distribute among your users.

WARNING! You can only send the package to Security Agents that report to the server where the package was created. Do not send the package to Security Agents that report to other Trend Micro Security Servers.

Installing with an MSI File

If you are using Active Directory, you can install the Security Agent by creating a Microsoft Windows Installer file. Use Client Packager to create a file with an `.msi` extension. You can take advantage of Active Directory features by automatically deploying the Agent to all clients simultaneously with the MSI file, rather than requiring each user to install the Security Agent themselves.

For more information on MSI, see the Microsoft website. For instructions on creating an MSI file, see [Installing with Client Packager](#) on page 3-9.

Installing with Remote Install

You can remotely install the Security Agent to multiple Windows 7, Vista, XP (Professional Edition only), Server 2003, Server 2008, SBS 2008, and EBS 2008 computers at the same time.

Note: To use Remote Install, you need administrator rights on the target computers. For Windows 7, Vista, Server 2008, SBS 2008, and EBS 2008, you will need to use a built-in domain administrator password because of Windows User Account Control (UAC). Turn off UAC in order to use a non-built-in administrator account.

To install the SA with Remote Install:

Note: Installing Security Agents on Windows Vista requires a few additional steps. See [*Enabling Security Agent Remote Install on Windows Vista/7 Clients*](#) on page 3-13.

1. From the Web Console main menu, click **Security Settings > Add**. The **Add Computer** screen appears.
2. Select **Desktop or Server**, from the **Computer Type** section.
3. Select **Remote Install**, from the **Method** section.
4. Click **Next**. The **Remote Install** screen appears.
5. From the list of computers in the **Groups and Computers** box, select a client, and then click **Add**. A prompt for a user name and password to the target computer appears.
6. Type your user name and password, and then click **Login**. The target computer appears in the **Selected Computers** list box.
7. Repeat these steps until the list displays all the Windows computers in the **Selected Computer** list box.
8. Click **Install** to install the Security Agent to your target computers. A confirmation box appears.
9. Click **Yes** to confirm that you want to install the Agent to the client. A progress screen appears as the program copies the Security Agent files to each target computer.

When WFBS completes the installation to a target computer, the installation status will appear in the **Result** field of the selected computers list, and the computer name appears with a green check mark.

Note: Remote Install will not install the Security Agent on a machine already running a Trend Micro Security Server.

Enabling Security Agent Remote Install on Windows Vista/7 Clients

Installing Security Agents on Windows Vista clients requires additional steps.

To enable Remote Install on Windows Vista Clients:

1. On the client, temporarily enable File and Printer Sharing.

Note: If the company security policy is to disable Windows Firewall, proceed to step 2 to start the Remote Registry service.

- a. Open Windows Firewall in the Control Panel.
 - b. Click **Allow a program through Windows Firewall**. If you are prompted for an Administrator password or confirmation, type the password or provide confirmation. The Windows Firewall Settings window appears.
 - c. Under the **Program or port list** in the **Exceptions** tab, make sure the **File and Printer Sharing** check box is selected.
 - d. Click **OK**.
2. Temporarily start the Remote Registry service.
 - a. Open Microsoft Management Console.

Tip: Type `services.msc` in the Run window to open Microsoft Management Console.

- b. Right-click **Remote Registry** and select **Start**.
3. If required, return to the original settings after installing Security Agents on the Windows Vista Client.

Installing with Vulnerability Scanner

Use Trend Micro Vulnerability Scanner (TMVS) to detect installed antivirus solutions, search for unprotected computers on your network, and install the Security Agent on them. To determine if computers need protection, Vulnerability Scanner pings ports that antivirus solutions normally use.

This section explains how to install the Agent with Vulnerability Scanner. For instructions on how to use Vulnerability Scanner to detect antivirus solutions, see [Verifying Client Installation with Vulnerability Scanner](#) on page 3-18.

Note: You can use Vulnerability Scanner on machines running Windows Server 2003; however, the machines should not be running Terminal Server. You cannot install the Security Agent on a client with Vulnerability Scanner if an installation of the Trend Micro Security Server is present on the client.

To install the Security Agent with Vulnerability Scanner:

1. In the drive where you installed the Trend Micro Security Server, go to the following location: **{server location} > PCCSRV > Admin > Utility > TMVS**. Double-click **TMVS.exe**. The **Trend Micro Vulnerability Scanner** console appears.
2. Click **Settings**. The **Settings** screen appears.

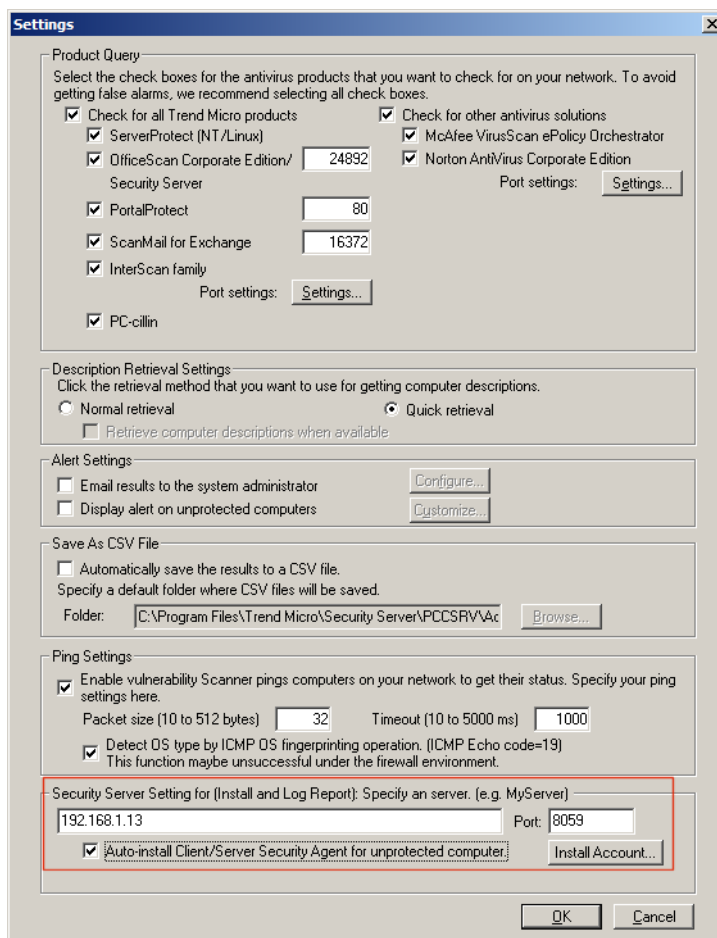


FIGURE 3-1. TMVS Settings screen

3. Under **Trend Micro Security Server Setting (for Install and Log Report)**, type the Trend Micro Security Server name or IP address and port number.
4. Select the **Auto-install Security Agent for unprotected computer** check box.
5. Click **Install Account**.

6. Type a user name and password with Administrator privileges to the server (or domain), and then click **OK**.
7. Click **OK** to go back to the main TMVS screen.
8. Click **Start** to begin checking the computers on your network and begin the Security Agent installation.

Installing with Email Notification

Navigation Path: Security Settings > Add

Use this to send an email message with a link to the installer.

To notify the location of the package from the console:

1. From the Web Console main menu, click **Security Settings > Add**. The Add Computer screen appears.
2. Select **Desktop** or **Server**, from the **Computer Type** section.
3. Select **Email notification install**, from the **Method** section.
4. Click **Next**. The **Email Notification Install** screen appears.
5. Type the subject of the email and the recipients.
6. Click **Apply**. The default email client opens with recipients, subject, and the link to the installer.

Installing MSA from the Web Console (Advanced only)

The Messaging Security Agent (MSA) can also be installed from the Web Console.

To install the MSA from the Web Console:

1. Log on to the Web Console.
2. Click the **Security Settings** tab, and then click the **Add** button.
3. Under the **Computer Type** section, click **Microsoft Exchange server**.

4. Under **Microsoft Exchange Server Information**, type the following information:
 - **Server name:** The name of the Microsoft Exchange server to which you want to install MSA.
 - **Account:** The built-in domain administrator user name.
 - **Password:** The built-in domain administrator password.
5. Click **Next**. The **Microsoft Exchange Server Settings** screen appears.
6. Under **Web Server Type**, select the type of Web server that you want to install on the Microsoft Exchange server. You can select either **IIS Server** or **Apache Server**.
7. For the **Spam Management Type**, **End User Quarantine** will be used.
8. Under **Directories**, change or accept the default target and shared directories for the MSA installation. The default target and shared directories are C:\Program Files\Trend Micro\Messaging Security Agent and C\$, respectively.
9. Click **Next**. The **Microsoft Exchange Server Settings** screen appears again.
10. Verify that the Microsoft Exchange server settings that you specified in the previous screens are correct, and then click **Next** to start the MSA installation.
11. To view the status of the MSA installation, click the **Live Status** tab.

Verifying the Agent Installation, Upgrade, or Migration

After completing the installation or upgrade, verify that the Security Agent is properly installed.

To verify the installation:

- Look for the WFBS program shortcuts on the Windows **Start** menu of the client running the Agent.
- Check if WFBS is in the **Add/Remove Programs** list of the client's Control Panel.
- Use Vulnerability Scanner (see [Verifying Client Installation with Vulnerability Scanner](#) on page 3-18).
- Use the Client Mover tool.

Verifying Client Installation with Vulnerability Scanner

Verify all the clients in the network have Agents installed. Automate the Vulnerability Scanner by creating scheduled tasks. For information on how to automate Vulnerability Scanner, see the WFBS online help.

Note: You can use Vulnerability Scanner on machines running Server 2003; however, the machines should not be running Terminal Server.

To verify Agent installation using Vulnerability Scanner:

1. In the drive where you installed the Trend Micro Security Server, go to . . . \Trend Micro Security Server\PCCSRV\Admin\Utility\TMVS. Double-click TMVS.exe. The **Trend Micro Vulnerability Scanner** console appears.
2. Click **Settings**. The **Settings** screen appears.
3. Under **Product Query**, select the **OfficeScan Corporate Edition/Worry-Free Business Security** check box and specify the port that the server uses to communicate with clients.
4. Under **Description Retrieval Settings**, click the retrieval method to use. Normal retrieval is more accurate, but it takes longer to complete.

If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting the **Retrieve computer descriptions when available** check box.
5. To have results automatically sent to you or to other Administrators in your organization, select the **Email results to the system administrator** check box under **Alert Settings**. Then click **Configure** to specify your email settings.
 - In **To**, type the email address of the recipient.
 - In **From**, type your email address.
 - In **SMTP server**, type the address of your SMTP server. For example, type smtp.example.com. The SMTP server information is required.
 - In **Subject**, type a new subject for the message or accept the default subject.
6. Click **OK** to save your settings.
7. To display an alert on unprotected computers, click the **Display alert on unprotected computers** check box. Then click **Customize** to set the alert message. The **Alert Message** screen appears.

8. Type a new alert message in the text box or accept the default message and then click **OK**.
9. To save the results as a comma-separated value (CSV) data file, select the **Automatically save the results to a CSV file** check box. By default, Vulnerability Scanner saves CSV data files to the TMVS folder. If you want to change the default CSV folder, click **Browse**, select a target folder on your computer or on the network, and then click **OK**.
10. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout fields**.
11. Click **OK**. The **Vulnerability Scanner** console appears.
12. To run a manual vulnerability scan on a range of IP addresses, do the following:
 - a. In **IP Range to Check**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers.
 - b. Click **Start** to begin checking the computers on your network.
13. To run a manual vulnerability scan on computers requesting IP addresses from a DHCP server, do the following:
 - a. Click the **DHCP Scan** tab in the **Results** box. The **DHCP Start** button appears.
 - b. Click **DHCP Start**. Vulnerability scanner begins listening for DHCP requests and performing vulnerability checks on clients as they log on to the network.

Vulnerability Scanner checks your network and displays the results in the **Results** table. Verify that all servers, desktops, and portable computers have the Agent installed.

If Vulnerability Scanner finds any unprotected servers, desktops, or portable computers, install the Agent on them using your preferred Agent installation method.

Verifying Client-Server Connectivity

Worry-Free Business Security represents the Client connection status in the Security Groups Tree using icons. However, certain conditions may prevent the Security Groups Tree from displaying the correct Client connection status. For example, if the network cable of a Client is accidentally unplugged, the Client will not be able to notify the Trend Micro Security Server that it is now offline. This Client will still appear as online in the Security Groups Tree.

You can verify client-server connection manually or schedule the verification from the Web Console.

Verify Connection does not allow the selection of specific groups or Clients. It verifies the connection to all Clients registered with the Security Server.

Testing the Client Installation with the EICAR Test Script

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

Obtaining the EICAR Test File:

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

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

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

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

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

Removing Agents

There are two ways to remove Agents:

- Running the Agent uninstallation program
- Using the Web Console

Removing the SA Using the Agent Uninstallation Program

If you granted users the privilege to remove the Agent, instruct them to run the Agent uninstallation program from their computer.

To run the Agent uninstallation program:

1. On the Windows **Start** menu, click **Settings > Control Panel > Add or Remove Programs**.
2. Select **Trend Micro Security Agent** and click **Change/Remove**. The **Security Agent Uninstallation** screen appears and prompts for the uninstall password, if configured.
3. Type the uninstall password and then click **OK**.

Removing the SA Using the Web Console

You can also remotely remove the Security Agent using the Web Console.

To remotely remove an Agent using the Web Console:

1. Log on to the Web Console.
2. Click the **Security Settings** tab.
3. In the Security Groups tree, select the client from which you want to remove the Agent and then click **Remove**. The **Remove Computer** screen appears.
4. Under **Removal Type**, click **Uninstall the selected agents**, and then click **Apply**. A confirmation message appears.
5. Click **OK**. A popup screen appears and displays the number of uninstall notifications that were sent by the server and received by the client.
6. Click **OK**.

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

Removing the Agent from Exchange Servers (Advanced only)

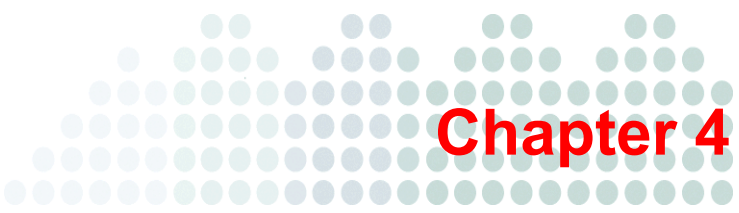
To remove a Messaging Security Agent using the Web Console:

1. Log on to the Microsoft Exchange Server with Administrator rights.
2. On the Microsoft Exchange Server, click **Start** and then **Control Panel**.
3. Open **Add or Remove Programs**.
4. Select **Trend Micro** Messaging Security Agent and click **Remove**. Follow the on-screen instructions.

Running the Messaging Security Agent Uninstallation Program (Advanced only)

To remove the Messaging Security Agent:

1. Log on to the Microsoft Exchange Server with Administrator rights.
2. On the Microsoft Exchange Server, click **Start** and then **Control Panel**.
3. Open **Add or Remove Programs**.
4. Select **Trend Micro** Messaging Security Agent and click **Remove**. Follow the on-screen instructions.



Chapter 4

Managing Groups

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

The topics discussed in this chapter include:

- *Groups* starting on page 4-2
- *Adding Groups* starting on page 4-4
- *Adding Clients to Groups* starting on page 4-5
- *Moving Clients* starting on page 4-5
- *Replicating Group Settings* starting on page 4-6
- *Importing and Exporting Settings* starting on page 4-6
- *Removing Computers from the Web Console* starting on page 4-7
- *Removing Inactive Security Agents* on page 4-8

Groups

Navigation Path: Security Settings > {group}

In WFBS, groups are a collection of computers and servers (not including Microsoft Exchange servers) that share the same configuration and run the same tasks. By grouping clients, you can simultaneously configure and manage multiple Agents.

For ease of management, group clients based on the departments to which they belong or the functions they perform. Also, group clients that are at a greater risk of infection to apply a more secure configuration to all of them in just one setting. Microsoft Exchange servers cannot be grouped together.

By default, the Security Server assigns clients to groups (desktops, servers, or Exchange servers) based on the type of Agent that is installed and the operating system on which the Agent is installed.

From the **Security Settings** screen, you can manage all clients on which you installed Security Agents and Messaging Security Agents and customize your security settings for Agents.

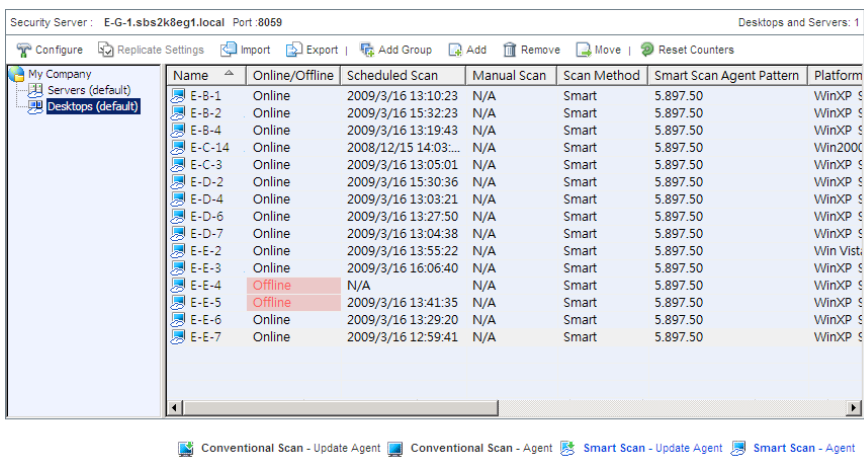


FIGURE 4-1. Security Settings screen showing clients in a group

Clients are displayed according to their group in the Security Groups tree. The Security Groups tree is an expandable list of logical groups of clients.

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

Tip: To select multiple, adjacent clients, click the first computer in the range, hold down the SHIFT key, and then click the last computer in the range. To select a range of non-contiguous clients, click the first computer in the range. Hold down the CTRL key and then click the clients you want to select.

Note: (Advanced only) Microsoft Exchange servers with Messaging Security Agents installed are registered to the servers group. However, they are displayed individually in the Security Groups tree; they cannot be grouped together.

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

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

From here you can:

- **Configure groups:** See [Adding Groups](#) on page 4-4.
- **Replicate settings from one group to another:** See [Replicating Group Settings](#) on page 4-6.
- **Add new clients:** See [Adding Clients to Groups](#) on page 4-5
- **Remove clients:** See [Removing Computers from the Web Console](#) on page 4-7
- **Import/Export settings:** See [Importing and Exporting Settings](#) on page 4-6
- **Add new groups:** See [Adding Groups](#) on page 4-4.
- **Remove groups:** See [Removing Computers from the Web Console](#) on page 4-7.
- **Move Clients from one Group to another or one Security Server to another:** See [Moving Clients](#) on page 4-5.

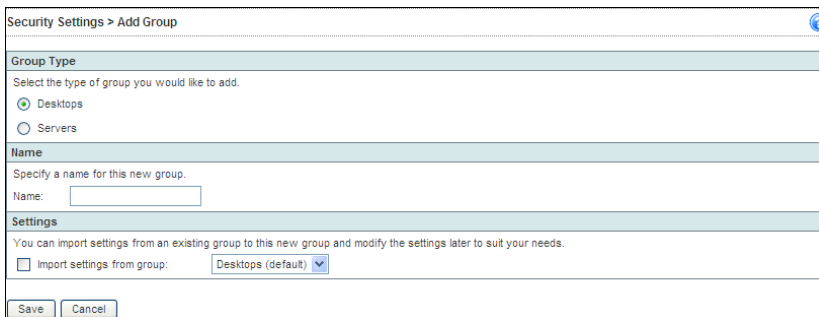
- **Reset counters:** Click **Reset Counters** on the **Security Settings Toolbar**. Resets the spam, virus/malware, spyware/grayware, and URL violation incidents.

Adding Groups

Navigation Path: Security Settings > Add Group

Create groups to collectively manage multiple clients.

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



The screenshot shows the 'Security Settings > Add Group' window. It has a title bar with a help icon. The window is divided into sections: 'Group Type' with radio buttons for 'Desktops' (selected) and 'Servers'; 'Name' with a text input field and a label 'Name:'; and 'Settings' with a checkbox 'Import settings from group:' and a dropdown menu currently set to 'Desktops (default)'. At the bottom are 'Save' and 'Cancel' buttons.

FIGURE 4-2. Add Group screen

To add a group:

1. From the **Add Group** screen, update the following as required:
 - **Group Type:** Select either Desktop or Server.
 - **Import settings from group:** Imports the security settings from the selected group.
2. Click **Save**.

Adding Clients to Groups

Navigation Path: Security Settings > Add

See *Installing Security Agents to Desktops and Servers* on page 3-2

Moving Clients

Navigation Path: Security Settings > {group}

WFBS gives you the option to move clients from one Group to another or one Security Server to another.

The screenshot shows a web-based interface for moving desktops or servers. At the top, a breadcrumb trail reads 'Security Settings > Move Desktop/Server'. Below this is a header bar labeled 'Move Desktop/Server'. The main content area contains the instruction: 'Move selected desktop(s) or server(s) on-line to another Security Server. Enter the new server name and port number below.' There are two input fields: 'Server name:' and 'Port:'. At the bottom left, there are two buttons: 'Move' and 'Cancel'. A help icon is visible in the top right corner of the dialog.

FIGURE 4-3. Move Desktop/Server screen

To move a Client from one Group to another:

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

To move a Client from one Security Server to another:

1. From the **Security Settings** screen, select the **Group**, and then select the client.
2. Click **Move**.
3. Type the new server name and port number. You can obtain the port number on the Security Settings screen by clicking on a server (see *Figure 4-1. Security Settings screen showing clients in a group*). The port number appears at the top.
4. Click **Move**.

Replicating Group Settings

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

Navigation Path: Security Settings > {group} > Replicate Settings

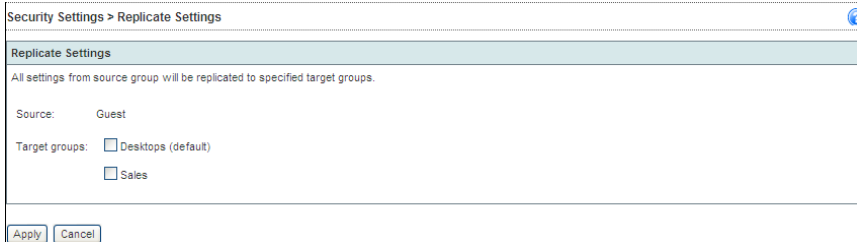


FIGURE 4-4. Replicate Settings screen

To replicate settings from one group to another:

1. From the **Security Settings** screen, select the source Group that must replicate its settings to other Groups.
2. Click **Replicate Settings**.
3. Select the target groups that must inherit the settings from the source Group.
4. Click **Apply**.

Importing and Exporting Settings

Navigation Path: Security Settings > {group} > Import or Export

You can save the settings for your desktop and server groups and then later imported them for new desktops and servers. The settings are saved as a .dat file. The following settings can be imported and exported:

- **In Security Settings:**

Antivirus/Anti-Spyware, Firewall, Web Reputation, URL Filtering, Behavior Monitoring, Tools, Client Privilege, Quarantine

- **In Scans:**

Manual Scan, Scheduled Scan

Note: You can import/export settings between desktop and server groups. Settings are not dependent on group type.

To import settings:

1. On the **Security Settings** screen, select a group.
2. Click **Import**. The Import Settings screen appears.
3. Click **Browse**, find the file, and then click **Import**.

To export settings:

1. On the **Security Settings** screen, select a group.
2. Click **Export**. The Export Settings screen appears.
3. Click **Export**.

On the Windows dialog box, click Save and select the location. To export the settings to one or more domain that this server also manages, use **Replicate Settings**.

Removing Computers from the Web Console

Navigation Path: Security Settings > {computer} > Remove

You can use Remove to accomplish two goals:

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

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

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

To remove a Client or group:

1. Click the computer (SA or MSA) that you want to remove.
2. Click **Remove** from the toolbar.
 - Select **Remove the selected agent(s)** to remove the client icon from the Web Console.
 - Select **Uninstall the selected agent(s)** to remove the Security Agent from the selected computers and remove the computer icons from the Web Console.
3. Click **Apply**.

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

Removing Inactive Security Agents

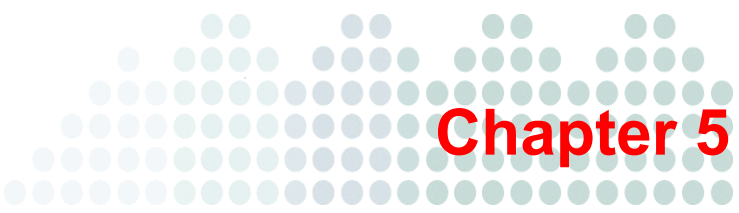
When you use the Security Agent uninstallation program on the Client to remove the Agents from a computer, the program automatically notifies the Security Server. When the Security Server receives this notification, it removes the Client icon from the Security Groups Tree to show that the Client does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

However, if the Security Agent is removed using other methods, such as

- reformatting the computer's hard drive
- deleting the Client files manually
- removing the Security Agent when the Client is not connected to the network

the Security Server will not be aware of the removal and it will display the Security Agent as inactive. If a user unloads or disables the Agent for an extended time, the Security Server also displays the Security Agent as inactive.

To have the Security Groups Tree only display active Clients, you can configure the Security Server to remove inactive Security Agents from the Security Groups Tree automatically.



Chapter 5

Managing Basic Security Settings

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

Options for Desktop and Server Groups on page 5-2

Configuring Real-time Scan on page 5-4

Managing the Firewall on page 5-4

Web Reputation on page 5-13

URL Filtering on page 5-16

Behavior Monitoring on page 5-17

Device Control on page 5-20

User Tools on page 5-22

Configuring Client Privileges on page 5-23

Configuring the Quarantine on page 5-25

Options for Desktop and Server Groups

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

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

TABLE 5-1. Configuration Options for Desktop and Server Groups

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

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

Configuring Real-time Scan

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

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

Managing the Firewall

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

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

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

Default Firewall Simple Mode Settings

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

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

TABLE 5-2. Default Firewall Settings

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

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

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

LOCATION	FIREWALL SETTINGS
In Office	Off
Out of Office	Off

Traffic Filtering

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

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

Scanning for Network Viruses

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

Stateful Inspection

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

Common Firewall Driver

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

Configuring the Firewall

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

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

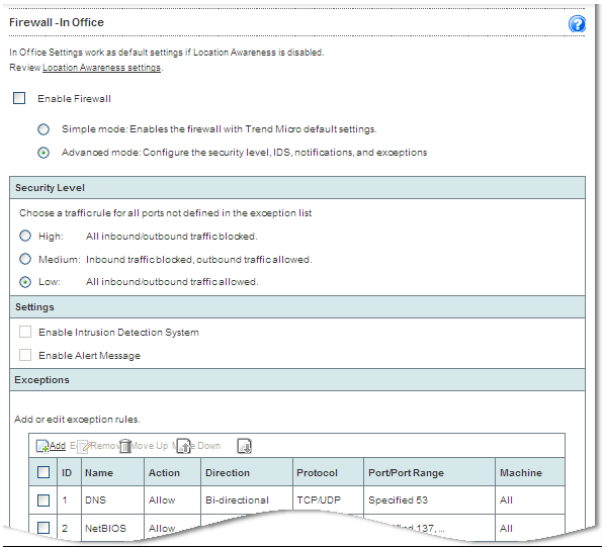


FIGURE 5-1. Firewall - In Office screen

Trend Micro default setting

- Firewall disabled

To configure the Firewall:

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

Advanced Firewall Options

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

To configure advanced firewall options:

1. From the **Firewall** screen, select **Advanced Mode**.
2. Update the following options as required:
 - **Security Level:** The security level controls the traffic rules to be enforced for ports not in the exception list.
 - **High:** blocks all incoming and outgoing traffic except any traffic allowed in the exception list.
 - **Medium:** blocks all incoming traffic and allows all outgoing traffic except any traffic allowed and blocked in the exception list.
 - **Low:** allows all incoming and outgoing traffic except any traffic blocked in the exception list. This is the default setting for the Simple mode.
 - Settings
 - **Enable Intrusion Detection System:** Intrusion Detection System identifies patterns in network packets that may indicate an attack. See [Intrusion Detection System](#) on page 5-11.
 - **Enable Alert Messages:** When WFBS detects a violation, the client is notified.
 - **Exceptions:** Ports in the exception list will not be blocked. See [Working with Firewall Exceptions](#) on page 5-9.
3. Click **Save**.

Working with Firewall Exceptions

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

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

Adding/Editing Exceptions

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

To add an Exception:

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

To edit an Exception:

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

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

Editing Exceptions

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

To edit an exception:

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

3. Update the options as required. See *Adding/Editing Exceptions* on page 5-9.
4. Click **Save**.

Removing Exceptions

To remove an exception:

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

Disabling the Firewall

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

To disable the Firewall:

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

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

Intrusion Detection System

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

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

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

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

Stateful Inspection

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

Web Reputation

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

or, for Advanced:

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

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

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

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

Reputation Score

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

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

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

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

Configuring Web Reputation

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

or, for Advanced:

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

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

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

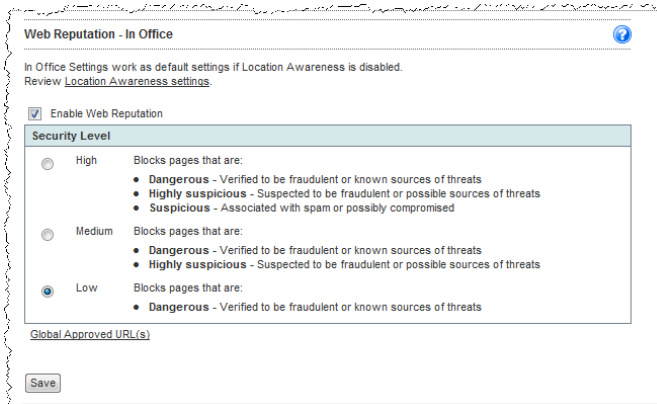


FIGURE 5-2. Web Reputation screen

To edit Web Reputation settings:

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

URL Filtering

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

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

URL Filtering 

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

☒ Enable URL Filtering

Filter Strength

☐ High Blocks known or potential security threats, inappropriate or possibly offensive content, content that can affect productivity or bandwidth, and unrated pages
☒ Medium Blocks known security threats and inappropriate content
☐ Low Blocks known security threats
☐ Custom Select specific page categories to block

Filter Rules

URL Category	☐ Business Hours	☐ Leisure Hours
 Adult	☒	☐
 Business	☐	☐

FIGURE 5-3. URL Filtering screen

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

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

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

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

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

Behavior Monitoring

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

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

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

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

Behavior Monitoring

Behavior Monitoring detects unidentified malware and proactively stops it from making changes. It also protects specified folders from unauthorized modification.

☒ Enable Behavior Monitoring

☐ Enable Intuit QuickBooks Protection

☒ Enable Malware Behavior Blocking

Exceptions

Programs in the approved list are not monitored for suspicious behavior, while programs in the blocked list are automatically blocked.

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

Add to Approved List

Add to Blocked List

Approved Program List

Name	Program Full Path

Blocked Program List

Name	Program Full Path

Save

FIGURE 5-4. Behavior Monitoring screen

To edit Behavior Monitoring settings:

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

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

5-18

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

The following products are supported:

QuickBooks Simple Start

QuickBooks Pro

QuickBooks Premier

QuickBooks Online

- **Enable Malware Behavior Blocking:** A group of technologies based on rule sets that attempt to identify certain suspicious behaviors that are common amongst malware or Fake Anti-Virus. Examples of such behaviors may include sudden and unexplainable new running services, changes to the firewall, system file modifications, etc.
- **Exceptions:** Exceptions include an **Approved Program List** and a **Blocked Program List**: Programs in the **Approved Programs List** can be started even if it violates a monitored change, while programs in the **Blocked Program List** can never be started.
 - **Enter Program Full Path:** Type the full Windows or UNC path of the program. Separate multiple entries with semicolons. Click **Add to Approved List** or **Add to Blocked List**. Use environment variables to specify paths, if required. See [Table 5-3](#) on page 5-20 for the list of supported variables.
 - **Approved Program List:** Programs (maximum of 100) in this list can be started. Click the corresponding  icon to delete an entry.
 - **Blocked Program List:** Programs (maximum of 100) in this list can never be started. Click the corresponding  icon to delete an entry.

2. Click **Save**.

Environment Variables

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

TABLE 5-3. Supported Variables

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

Device Control

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

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

Set the following as required:

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

TABLE 5-4. Device Control Permissions

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

- **Exceptions:** If a user is not given read permission for a particular device, the user will still be allowed to run or open any file or program in the Approved List. However, if AutoRun prevention is enabled, even if a file is included in the Approved List, it will still not be allowed to run.
To add an exception to the Approved List, enter the file name including the path or the digital signature and click **Add to the Approved List**

User Tools

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

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

Anti-Spam Toolbar Requirements

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

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

The Anti-Spam toolbar supports the following operating systems:

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

Configuring User Tools

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

To edit the availability of User tools:

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

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

2. Click **Save**.

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

Configuring Client Privileges

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

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

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

Configuring Client Privileges

Client Privileges

Grant clients the privilege to modify the following settings:

Antivirus/Anti-spyware
☐ Real-time Scan settings ☐ Manual Scan settings ☐ Scheduled Scan settings ☐ Skip Scheduled Scan
Firewall
☐ Firewall settings
Web Reputation
☐ Continue browsing malicious URLs until computer restart
URL Filtering
☐ Continue browsing restricted URLs until computer restart
Behavior Monitoring
☐ Behavior Monitor Settings
Proxy Settings
☒ Allow users to configure proxy settings (Disabling this feature will reset the proxy settings to their default)
Update Privileges
☒ Allow users to perform manual Update ☒ Use Trend Micro ActiveUpdate as a secondary update source ☐ Disable Agent upgrade and hotfix deployment. (Check this box to disable Agent upgrade. Pattern updates will still be applied. Clear this box to perform an upgrade.)
Client Security
☒ Prevent users or other processes from modifying Trend Micro program files, registries and processes

Save

FIGURE 5-5. Client Privileges screen

To grant privileges to Clients:

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

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

2. Click **Save**.

Configuring the Quarantine

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

The default folder on the client is:

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

The default folder on the server is:

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

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

Configuring the Quarantine Directory

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

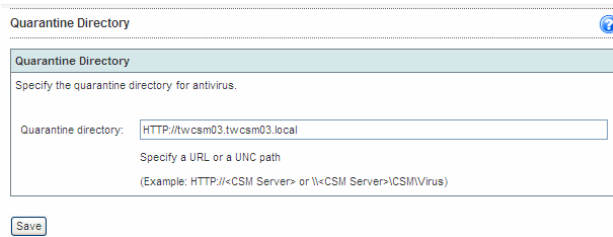
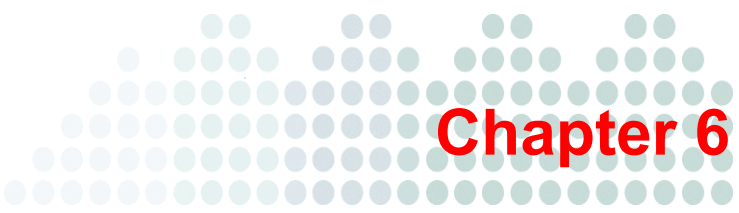


FIGURE 5-6. Quarantine Directory screen

To set the Quarantine directory:

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



Chapter 6

Managing Scans

This chapter describes how to use Smart Scan, Conventional Scan, and Manual and Scheduled scans to protect your network and clients from virus/malware and other threats.

The topics discussed in this chapter include:

- *About Scanning* on page 6-2
- *Enabling Real-Time Scanning* on page 6-4
- *Running Manual Scans on Desktops and Servers* on page 6-5
- *Running Scheduled Scans for Desktops and Servers* on page 6-7
- *Scheduling Scans* on page 6-9
- *Configuring Antivirus/Anti-Spyware Scans for Desktops and Servers* on page 6-10
- *Uncleanable Files* on page 6-16
- *Mail Scan* on page 6-17
- *Trojan Ports* on page 6-18

About Scanning

During a scan, the Trend Micro Virus 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, inert snippets of this code are captured in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match.

When the scan engine detects a file containing a virus or other malware, it executes an action such as clean, quarantine, delete, or replace with text/file (“replace” for Advanced only). You can customize these actions when you set up your scanning tasks.

WFBS provides three types of scans:

- Real-time Scan.
- Manual Scan (triggered either by the client or the server)
- Scheduled Scan

and two scan methods:

- Conventional Scan
- Smart Scan

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

Scan Types

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

- **Real-time Scan:** Real-time Scan is a persistent and ongoing scan. Each time a file is opened, downloaded, copied, or modified, Real-time Scan scans the file for threats. In the case of email messages (Advanced only), the Messaging Security Agent guards all known virus entry points with Real-time Scanning of all incoming messages, SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers.

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

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

- **Scheduled Scan:** A Scheduled Scan is similar to Manual Scan but scans all files and email messages at the configured time and frequency.
To configure a Scheduled scan, click **Scans > Scheduled Scan** (See [Scheduling Scans](#) on page 6-9 for more information).

Scan Methods

Client Scanning is performed in two different ways:

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

Note: In this implementation of WFBS, the Security Server acts as a Scan Server. The Scan Server is simply a service that runs on the Security Server. The Scan Server service is automatically installed during Security Server installation; there is no need to install it separately. If your clients are configured for Smart Scan but cannot connect to the Smart Scan service, they will attempt to connect to the Trend Micro Global Smart Scan Server.

Selecting the Scan Method

If client scans are slowing down client computers, switch to Smart Scan. By default, Smart Scan is enabled. You can disable Smart Scan for all groups and clients on the **Preferences > Global Settings > Desktop/Server > General Scan Settings** screen.

To select the scan method for individual groups:

1. Click **Security Settings > {group} > Configure > Scan Method**
2. Click **Smart Scan** or **Conventional Scan**.

Note: If your clients are configured for Smart Scan but cannot connect to the Scan Server on your network, they will attempt to connect to the Trend Micro Global Smart Scan Server.

Enabling Real-Time Scanning

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

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

WARNING! If you disable real-time scanning, Behavior Monitoring and Device Control are also disabled, and your desktops and servers become vulnerable to infected files.

To enable Real-time scanning on the Client:

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

Running Manual Scans on Desktops and Servers

Navigation Path: Scans > Manual

By default, Worry-Free Business Security sets your Clients to run Real-time scanning. You do not need to set any scanning options to protect your Clients.

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

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

The Manual Scan screen contains the following items:

- **Desktops (default)** (click the name to display options): Scans all Clients that belong to this group.
- **Servers (default)** (click the name to display options): Scans all server Clients that belong to this group.
- **[Name of Exchange Server]** (Advanced only) (Click the expand  icon to display more options): Select to have the Messaging Security Agent (MSA) scan email on the Microsoft Exchange server
 - Antivirus:** Select to have the MSA scan for viruses and other malware. Click to configure scan settings for the Antivirus feature.
 - Content Filtering:** Select to have the MSA scan email for prohibited content. Click to configure scan settings for the Content Filtering feature.
 - Attachment Blocking:** Select to have the MSA scan email for attachment rule violations. Click to configure scan settings for the Attachment Blocking feature.
- **Scan Now:** Starts the manual scan process. All items selected will be scanned.
- **Stop Scanning:** Stops the manual scan.

To run a manual scan:

1. Click **Scans > Manual Scan**. Accept the Trend Micro recommended default settings or customize your scan.
2. Select a group or groups to scan.

3. Click **Scan Now**. The Scan Notifying Progress screen appears. When the scan is complete the Scan Notifying Results screen appears to show you the results of the scan notifications.

Default Manual Scan settings recommended by Trend Micro:

- **Target**
 - **All scannable files:** Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.
 - **Scan compressed files up to 1 compression layers:** Scans compressed files that are 1 compression layers deep. Default is "off" for the default server group and "on" for the default desktop group.
- **Exclusions**
 - **Do not scan the directories where Trend Micro products are installed**
- **Advanced Settings**
 - **Scan boot area** (for Antivirus only)
 - **Modify Spyware/Grayware Approved List** (for Anti-spyware only)

Virus Pattern

The Trend Micro Virus Scan Engine uses an external data file, called the virus pattern file. It contains information that helps Worry-Free Business Security 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 website (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.

Note: Pattern file, scan engine, and database updates are only available to registered Worry-Free Business Security users under an active maintenance agreement.

Running Scheduled Scans for Desktops and Servers

Navigation Path: Scans > Scheduled Scans

The Scheduled Scan screen contains the following items:

- **Settings tab:** Select Clients to scan and choose scan options. Click the expand icon to display more options.
 - **Desktops (default)** (click the name to display options): Scans all Clients that belong to this group.
 - **Servers (default)** (click the name to display options): Scans all server Clients that belong to this group.
 - **[Name of Exchange Server]** (Advanced only) (Click the expand  icon to display more options): Select to have the Messaging Security Agent (MSA) scan email on the Microsoft Exchange server
 - Antivirus:** Select to have the MSA scan for viruses and other malware. Click to configure scan settings for the Antivirus feature.
 - Content Filtering:** Select to have the MSA scan email for prohibited content. Click to configure scan settings for the Content Filtering feature.
 - Attachment Blocking:** Select to have the MSA scan email for attachment rule violations. Click to configure scan settings for the Attachment Blocking feature.

- **Schedule tab:** Schedule one or more scans for one or more Clients.
 - **Daily:** Performs a scheduled scan every day.
 - **Weekly, every:** Performs a scheduled scan once a week. Select a day from the list.
 - **Monthly, on day:** Performs a scheduled scan once a month. Select a date from the list.

Regardless if you click **Daily**, **Weekly**, or **Monthly**, you must specify when to perform a scheduled scan in the Start time list boxes.

- **Save:** Remember to click **Save**.

Default Scheduled Scan settings recommended by Trend Micro:

- **Target**
 - **All scannable files:** Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.
 - **Scan compressed files up to 2 compression layers:** Scans compressed files that are 1 or 2 compression layers deep.
- **Exclusions**
 - **Do not scan the directories where Trend Micro products are installed**
- **Advanced Settings**
 - **Scan boot area** (for Antivirus only)
 - **Modify Spyware/Grayware Approved List** (for Anti-spyware only)

Scheduling Scans

Navigation Path: Scans > Scheduled > Schedule {tab}

Schedule scans to periodically scan clients and Microsoft Exchange servers (Advanced only) for threats.

Tip: Trend Micro recommends not scheduling a scan and an update to run at the same time. This may cause the Scheduled Scan to stop unexpectedly. Similarly, if you begin a Manual Scan when a Scheduled Scan is running, the Scheduled Scan will be interrupted. The Scheduled Scan aborts, but runs again according to its schedule.

Note: To disable Scheduled Scan, clear all options for the specific group or Microsoft Exchange server and click **Save**.

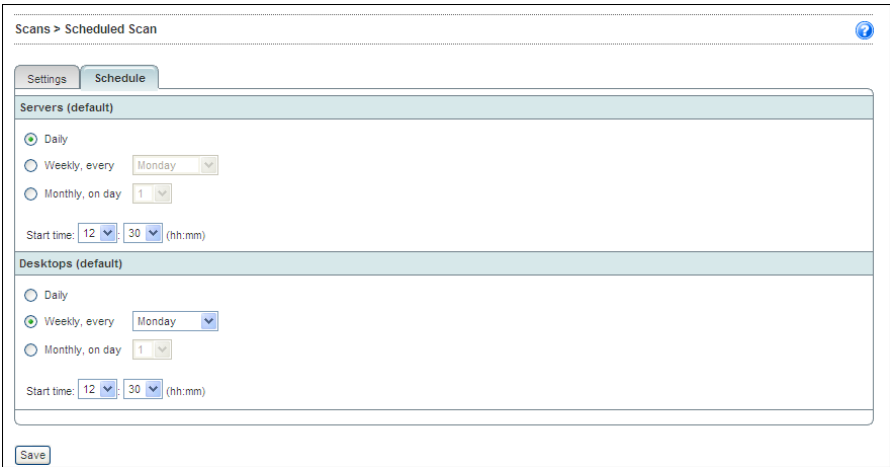


FIGURE 6-1. Scheduled Scan screen

To schedule a scan:

1. Before scheduling a scan, configure the settings for the scan. See [Running Scheduled Scans for Desktops and Servers](#) on page 6-7 and [Configuring Scan Options for Microsoft Exchange Servers](#) on page 9-7.
2. From the **Schedule** tab, update the following options for each group or Microsoft Exchange server (Advanced only) as required:
 - **Daily:** The Scheduled Scan runs every day at the **Start time**.
 - **Weekly, every:** The Scheduled Scan runs once a week on the specified day at the **Start time**.
 - **Monthly, on day:** The Scheduled Scan runs once a month on the specified day at the **Start time**. If you select 31 days and the month has only 30 days, WFBS will not scan the clients or Microsoft Exchange groups that month.
 - **Start time:** The time the Scheduled Scan should start.
3. Click **Save**.

Additionally, configure who receives notifications when an event occurs. See [Configuring Events for Notifications](#) on page 8-3.

Configuring Antivirus/Anti-Spyware Scans for Desktops and Servers

To customize scans, set the target files to scan, including the optional settings, and then set the actions for the Security Agent (SA) to take against detected threats.

For real time scans:

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

For Manual or Scheduled Scans:

Navigation Path: **Scans > {Manual or Scheduled} > {group} > Target {tab}**

Note: Disabling real-time scanning will also disable Behavior Monitoring and Device Control.

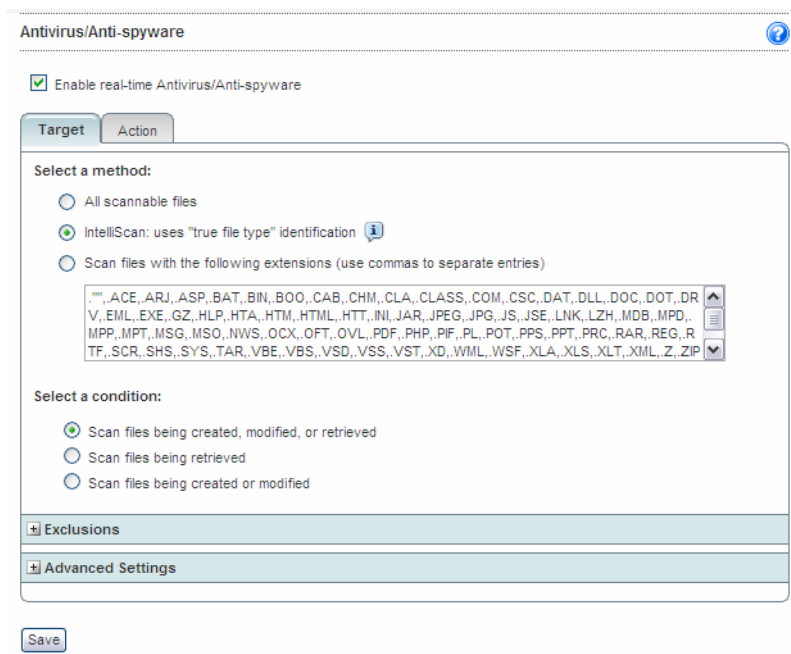


FIGURE 6-2. Configuring Antivirus/Anti-Spyware Scans

Set Target Files

To set the target files for the Security Agent to scan:

1. Under the **Target** tab, specify the files to scan.
 - **Select a method:**
 - **All scannable files:** includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions
 - **IntelliScan: uses “true file type” identification:** Scans files based on true-file type. (see [IntelliScan](#) on page D-4).
 - **Scan files with the following extensions:** Manually specify the files to scan based on their extensions. Separate multiple entries with commas.

- Scan mapped drives and shared folders on the network
 - Scan compressed files: Up to __ compression layers (up to 6 layers)
2. Click **Save**.

Exclusions

To set folders to exclude from scanning:

1. Click  to expand the Exclusions panel.
2. Select **Enable Exclusions**.
3. Set folders and files to exclude from scanning.
 - **Do not scan the following directories:** To exclude specific directories, type the directory names and click **Add**.
 - Select **Do not scan the directories where Trend Micro products are installed** to exclude all directories where Trend Products are installed.
 - **Do not scan the following files:** To exclude specific files, type the file names, or the file name with full path and click **Add**. All subdirectories in the directory path you specify will also be excluded.
 - **Do not scan files with the following extensions:** Specify the files to exclude based on their extensions. To use specified extensions, select the extensions to protect from the **Select file extension from the list**, and click **Add**.

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

To specify an extension that is not in the list, type it in the **Or type the extension below** text box and then click **Add**.

4. Click **Save**.

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

Advanced Settings

To configure Advanced Settings:

- **Scan POP3 Messages** (see [Mail Scan](#) on page 6-17)
- **Scan mapped drives and shared folders on the network:** select to scan directories physically located on other computers, but mapped to the local computer.
- **Scan floppy during system shutdown**
- **Enable IntelliTrap** (see [IntelliTrap](#) on page D-6)

Modify Spyware/Grayware Approved List

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

Worry-Free™ Business Security includes a list of potentially risky applications and, by default, prevents these applications from executing on Clients.

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

To add a spyware/grayware application to the approved list:

1. Under Advanced Settings, click the **Modify Spyware/Grayware Approved List** link.
2. Use the search function to locate the application name.
3. Select the application name in the left pane, and then click **Add**.
4. Click **Save**.

Set the actions for the SA to take against detected threats

Under the Action tab, Select one of the following action options:

1. **For Virus Detections:**
 - Select **ActiveAction** for Trend Micro recommended settings (See [ActiveAction](#) on page D-4).
 - Select **Customized action for the following detected threats:** to manually specify how to handle different types of detected threats.

- **Quarantine** is the default action for **Trojan, Spyware, and Packers**
 - **Clean** is the default action for **Viruses and Other Threats**
 - **Pass** is the default action for **Generic**
 - **Deny Access** (for real-time scans only)
 - **Delete** is the default action for cookies
2. For **Spyware Detections**:
- **Quarantine**
 - **Delete**
 - **Pass**
 - **Deny Access** (for Realtime scan only) - The Spyware/Grayware will remain on the computer, but will not be allowed to run
3. For **Advanced Settings**:
- Click  next to **Advanced settings** to expand the screen.
- **Display an alert message on the desktop or server when a virus/spyware is detected**
4. Click **Save**.
- Configure who receives notifications when an event occurs. See [Configuring Events for Notifications](#) on page 8-3.

Modifying the Spyware/Grayware Approved List

The Spyware/Grayware Approved List determines which spyware or grayware applications users can use. Only Administrators can update the list. See [Spyware/Grayware](#) on page 1-11.

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

Navigation Path: Scans > Manual Scan or Scheduled Scan > {group} > Advanced Settings > Modify Spyware/Grayware Approved List

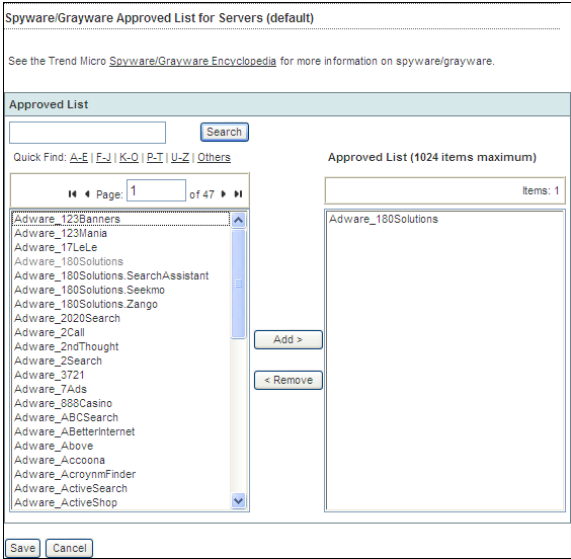


FIGURE 6-3. Spyware/Grayware Approved List screen

To update the Spyware/Grayware Approved List:

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

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

- **Right pane:** Approved spyware or grayware applications.

- **Add>:** Select the application name in the left pane and click **Add>**. To select multiple applications, press CTRL while clicking the application names.
3. Click **Save**.

Uncleanable Files

There are some situations when the Agent may not be able to clean files, even when the Virus Scan Engine and virus pattern file are up-to-date. By default, Worry-Free Business Security deletes files that cannot be cleaned.

Security Agents

Security Agents may not be able to clean the following:

- **Worms:** A computer worm is a self-contained program (or set of programs) 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. Worms are uncleanable because the file is a self-contained program.

Solution: Trend Micro recommends deleting worms.

- **Files on write-protected disks:** remove the write-protection to enable cleaning
- **Password-protected files:** remove the password-protection to enable cleaning
- **Backup files:** Files with the RB0~RB9 extensions are backup copies of infected files. Trend Micro Security creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.

Solution: If Trend Micro Security successfully cleans the infected file, you do not need to keep the backup copy. If the computer functions normally, you can delete the backup file.

- Files located in the Windows Recycle Bin, Windows Temp folder, or Internet Explorer temporary folder
- Files compressed using an unsupported compression format
- Locked files or files that are currently executing
- Corrupted files

Messaging Security Agents (Advanced only)

If the Messaging Security Agent is unable to successfully clean a file, it labels the file “uncleanable” and performs the user-configured action for uncleanable files. The default action is Delete entire message. The Messaging Security Agent records all virus events and associated courses of action in the log file.

Some common reasons why the Messaging Security Agent cannot perform the clean action are as follows:

- The file contains a Trojan, worm, or other malicious code. To stop an executable from executing, the Messaging Security Agent must completely remove it.
- The Messaging Security Agent does not support all compression forms. The scan engine only cleans files compressed using pkzip and only when the infection is in the first layer of compression.
- An unexpected problem prevents the Messaging Security Agent from cleaning, such as:
 - The temp directory that acts as a repository for files requiring cleaning is full
 - The file is locked or is currently executing
 - The file is corrupted
 - The file is password protected

Mail Scan

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

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

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

POP3 Mail Scan Requirements

POP3 Mail Scan supports the following mail clients:

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

Note: Mail Scan cannot detect security risks in IMAP messages. Use the Messaging Security Agent (Advanced only) to detect security risks and spam in IMAP messages.

To edit the availability of Mail Scan:

1. From the **Advanced Settings** screen, update the following as required:
 - **Scan POP3 Messages**
2. Click **Save**.

Trojan Ports

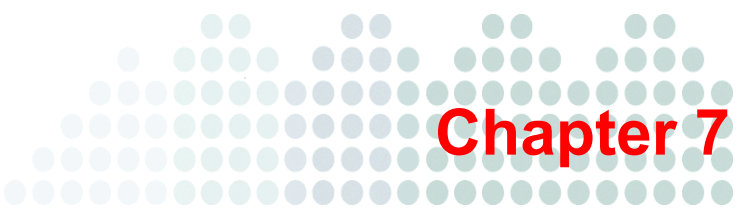
Trojan ports are commonly used by Trojan horse programs to connect to a computer. During an outbreak, Trend Micro Security blocks the following port numbers that Trojan programs may use:

TABLE 6-1. Trojan ports

PORT NUMBER	TROJAN HORSE PROGRAM	PORT NUMBER	TROJAN HORSE PROGRAM
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak

TABLE 6-1. Trojan ports (Continued)

PORT NUMBER	TROJAN HORSE PROGRAM	PORT NUMBER	TROJAN HORSE PROGRAM
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line



Chapter 7

Managing Updates

This chapter explains how to use and configure Manual and Scheduled Updates. Topics discussed in this chapter include:

- *Updating the Security Server* on page 7-2
- *Updating Security Agents* on page 7-3
- *Agent Update Sources* on page 7-5
- *Configuring Alternative Update Sources for Security Agents* on page 7-8
- *Update Agents* on page 7-10
- *Updatable Components* on page 7-18

Updating the Security Server

WFBS automatically performs the following updates:

- Security Server
 - When you install the product for the first time, all components for the Security Server are immediately updated from the Trend Micro ActiveUpdate server.
 - Whenever WFBS starts, the Security Server updates the components and the Outbreak Defense policy.
 - By default, Scheduled Updates run every hour. These updates are then pushed to all clients.
- Agents
 - When you install the product for the first time, all components for the clients are immediately updated from the Security Server.
 - By default, the Messaging Security Agent (Advanced only) runs a Scheduled update once every 24 hours at 12:00 AM.
 - In addition to updates being pushed to the Agents by the Security Server after the Security Server's hourly update, Agents also run a scheduled update every 8 hours (as an added check to ensure Agents are updated).

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

To configure Trend Micro Security Server to perform updates:

1. Select an update source. See [Configuring an Update Source for the SS and Agents](#) on page 7-5.
2. Configure the Trend Micro Security Server for manual or scheduled updates. See [Manually Updating Components](#) on page 7-15 and [Scheduling Component Updates](#) on page 7-16.

If you use a proxy server to connect to the Internet, ensure that you properly configure the proxy settings to download updates successfully. For more information, see [Internet Proxy Options](#) on page 11-3.

Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches, and service packs to address issues, enhance product performance, or add new features.

The following is a summary of the items Trend Micro may release:

- **Hot fix:** A workaround or solution to a single, customer-reported issue. Hot fixes are issue-specific, and therefore are not released to all customers. Windows hot fixes include a Setup program. Typically, stop the program daemons, copy the file to overwrite its counterpart in the installation, and restart the daemons.
- **Security Patch:** A hot fix focusing on security issues that is suitable for deployment to all customers. Windows security patches include a Setup program.
- **Patch:** A group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program.
- **Service Pack:** A consolidation of hot fixes, patches, and feature enhancements significant enough to be a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix, patch, and service pack releases:

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

All releases include a readme file with information needed to install, deploy, and configure the product. Read the readme file carefully before installing the hot fix, patch, or service pack files.

Updating Security Agents

To ensure that the Clients stay up-to-date, the Security Agent (SA) automatically performs the following updates:

- By default, the Security Server is updated every hour. The Scheduled Update is then pushed to all clients.
- In addition, Agents run a scheduled update every 8 hours (as an added check to ensure Agents are updated).

However, if you want to immediately update clients, you can do so using **Live Status > System Status > Component Updates > Deploy Now**.

Tip: To ensure that Security Agents stay up-to-date even when not connected to the Security Server, use Trend Micro ActiveUpdate as a secondary update (*Configuring an Update Source for the SS and Agents* on page 7-5). This is useful for end users who are often away from the office and disconnected from the local network.

To verify that client updates are successful, check the Update Logs. See *Using Log Query* on page 12-4.

To configure update and other options for clients, see *Configuring Client Privileges* on page 5-23

ActiveUpdate

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

Incremental updates of the pattern files

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

Using ActiveUpdate with WFBS

Click **Trend Micro ActiveUpdate Server** from the **Updates > Source** screen to set the Security Server to use the ActiveUpdate server as a source for manual and scheduled component updates. When it is time for a component update, the Security Server polls the ActiveUpdate server directly. If a new component is available for download, the Security Server downloads the component from the ActiveUpdate server.

Agent Update Sources

When choosing the Agent update locations, consider the bandwidth of the sections that are between clients and the update sources. The following table describes different component update options and recommends when to use them:

TABLE 7-1. Update Source Options

UPDATE SEQUENCE	DESCRIPTION	RECOMMENDATION
1. ActiveUpdate server 2. Security Server 3. Clients	The Trend Micro Security Server receives updated components from the ActiveUpdate server (or other update source) and deploys them directly to clients.	Use this method if there are no sections of your network between the Trend Micro Security Server and clients you identify as “low-bandwidth”.
1. ActiveUpdate server 2. Security Server 3. Update Agents 4. Clients	The Trend Micro Security Server receives updated components from the ActiveUpdate server (or other update source) and deploys them directly to Update Agents, which deploy the components to clients.	Use this method to balance the traffic load on your network if there are sections of your network between the Trend Micro Security Server and clients you identify as “low-bandwidth”.

Configuring an Update Source for the SS and Agents

Navigation Path: Updates > Source

The Update Source screen allows you to perform the following:

- Configure component update sources for the Security Server
- Set alternative update sources for Security Agents to download updated components

The Server Tab

During manual or scheduled downloads, the Security Server checks the location you have specified for the update source and downloads the latest components from that source. Once the Security Server has completed downloading the latest components, the clients download those components from the Security Server.

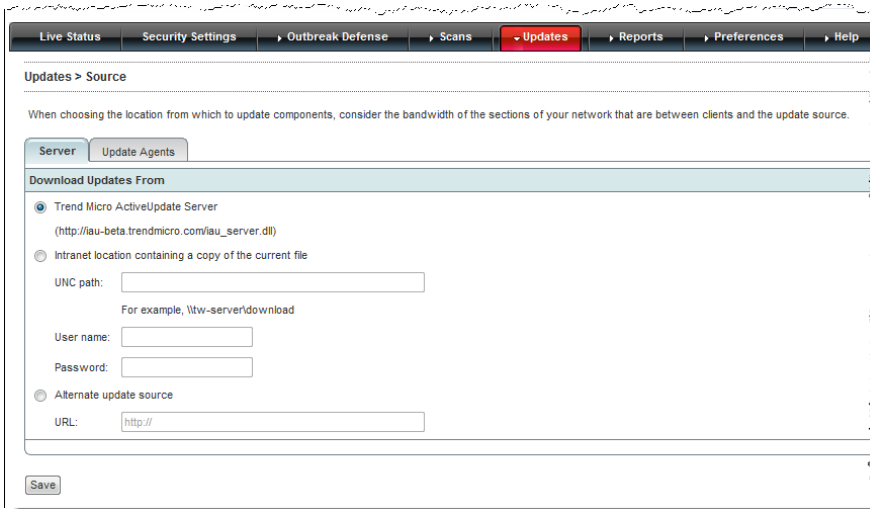


FIGURE 7-1. Update Source screen

To configure an update source for the Security Server:

1. From the **Source** screen, update the following options as required:
 - **Trend Micro ActiveUpdate Server:** Trend Micro ActiveUpdate Server is the Trend Micro default setting for the download source. Trend Micro uploads new components to the ActiveUpdate Server as soon as they are available.

Note: If you define a source other than the Trend Micro ActiveUpdate Server for receiving updates, then all servers receiving updates must have access to that source.

- **Intranet location containing a copy of the current file:** Download your components from an Intranet source that receives updated components. Type the Universal Naming Convention (UNC) path of another server on your network, and set up a directory on that target server as a shared folder available to all servers receiving the updates (for example, \\Web\\ActiveUpdate).
- **Alternate update source:** Download your components from an Internet or other source. Make the target HTTP virtual directory (Web share) available to all servers receiving the updates.

2. Click **Save**.

Update Agents Tab

- **Assign Update Agents:** Assigns Security Agents (SA) Update Agent privileges. Only other SAs can receive updated components from Update Agents. The Security Server cannot receive updated components from Update Agents.
- **Update Agents always update directly from the Security Server only:** This ensures that Update Agents will always download updated components from the Security Server instead of another Update Agent.
- **Alternative Update Sources:** Allows you to specify which Update Agents Security Agents use to get updated components.
 - **Enable alternative update sources for Security Agents and Update Agents:** You must have at least one Update Agent.
 - **Add:** Creates a new Alternative Update source entry. Select the Security Agent and port to be used as the new Update Agent (will be greyed out if no Update Agent has been assigned).

Tip: Tip: To ensure that the Security Agents (SA) download updates from an Update Agent, create two (2) entries with the same IP range and assign each entry a different Update Agent. If for some reason the first Update Agent is unavailable, the SA will attempt to download updates from the second Update Agent.

- **Remove:** Deletes an Alternative Update source entry (will be greyed out if no Update Agent has been assigned).

- **Reorder:** Reorders the IP addresses in the IP range list. IP addresses in the IP Range list are listed in the order that they were created. When the Security Server notifies an SA that updates are available, they scan the IP Range list to identify their correct update source. The SA scans the first item on the list and continues down the list until it identifies its correct update source (will be greyed out if no Update Agent has been assigned).

Configuring Alternative Update Sources for Security Agents

Navigation Path: Updates > Source

Security Agents can download components from a specified alternative update source. Using alternative update sources to deploy updated components can help to reduce network bandwidth consumption.

Each time you add an alternative update source, the source is added to an Update Source table. When new updates are available, the Security Agent scans each entry in the table, to identify the correct source.

Note: Security Agents that are not specified will automatically receive updates from the Trend Micro Security Server.

To add alternative update sources:

1. From the **Update Agents** tab on the **Source** screen, click **Add** in the **Alternative Update Sources** section.
2. Update the following options as required:
 - **IP from** and **IP to:** Clients with IP addresses within this range will receive their updates from the specified update source.

Note: To specify a single Security Agent, enter the Security Agent's IP address in both the **IP from** and **IP to** fields.

- Update source
 - **Update Agent:** If the drop-down list is not available, no Update Agents have been configured.

3. Click **Save**.

To remove an alternative update source, select the check box corresponding to the **IP Range** and click **Remove**.

Note: The Enable alternative update sources option must first be selected before Security Agents will start using alternative update sources.

To delete an alternative update source;

1. From the main navigation menu select **Updates > Source**. The Updates Source screen appears.
2. Click the **Update Agents** tab.
3. In the Alternative Update Sources table, select the check box in the first column that corresponds to the alternative update source(s) that you wish to delete.
4. Click **Remove**.

To reorder the alternative update source list:

1. From the main navigation menu select **Updates > Source**. The Updates Source screen appears.
2. Click the **Update Agents** tab.
3. In the **Alternative Update Sources** table, select the check box that corresponds to the IP address range(s) that you want to reorder.
4. Click **Reorder**. A blank text field appears in the Order column for each of the IP address ranges that you selected.
5. Type a value indicating the desired position of the IP address range within the IP address range list.

Note: If there are only three (3) IP addresses in the IP address range list, and you enter a value greater than 3, the item(s) you are reordering will be moved to the end of the IP address range table.

Update Agents

Update Agents are Security Agents (SA) that can receive updated components from the Security Server or ActiveUpdate Server and deploy them to other SAs.

Update Agents reduce network bandwidth consumption by eliminating the need for all SAs to access the Security Server for component updates.

TABLE 7-2. Update Agents.

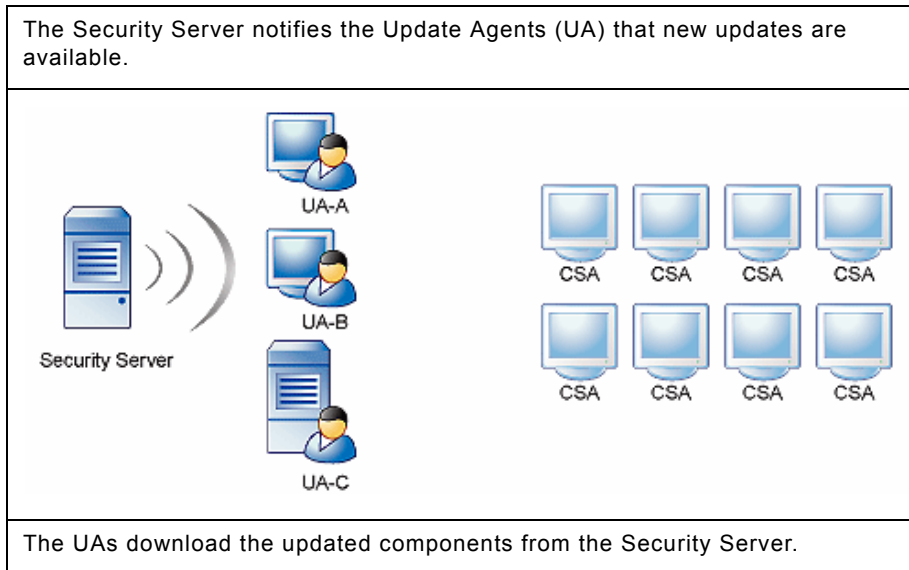


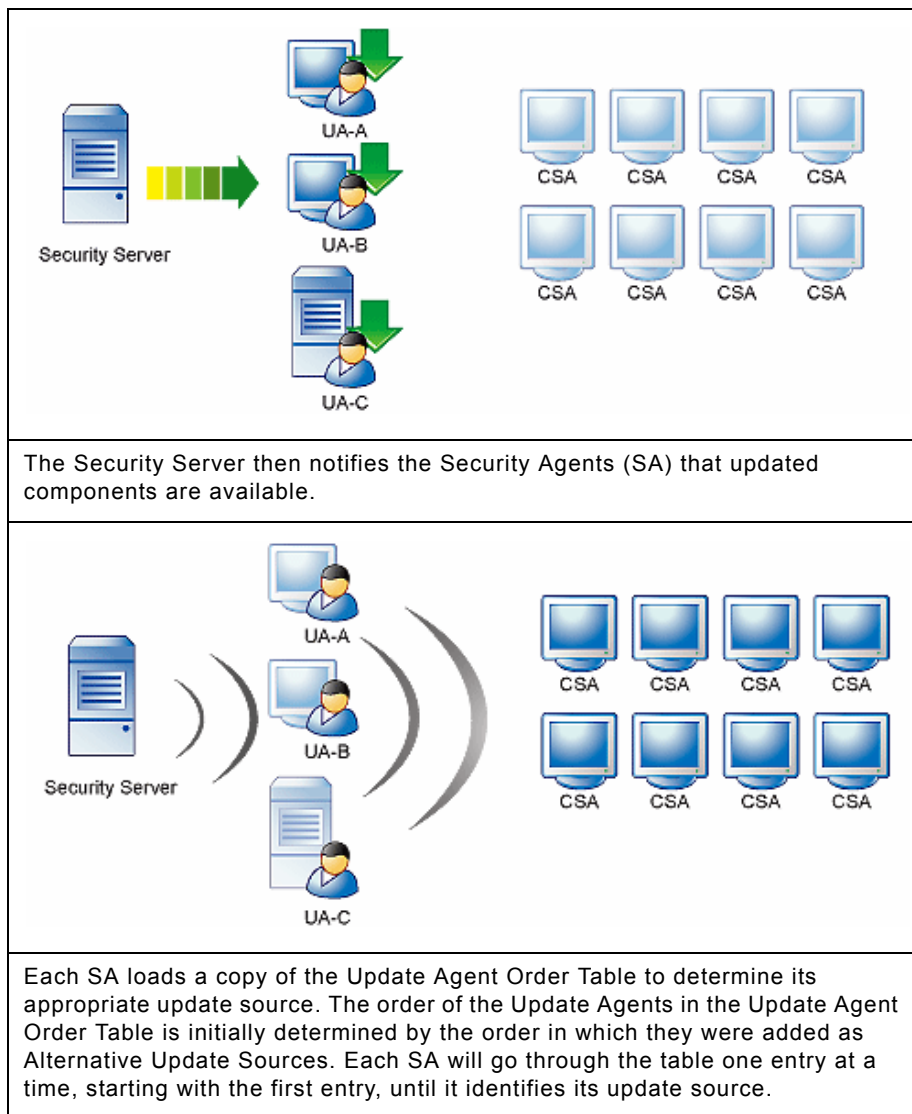
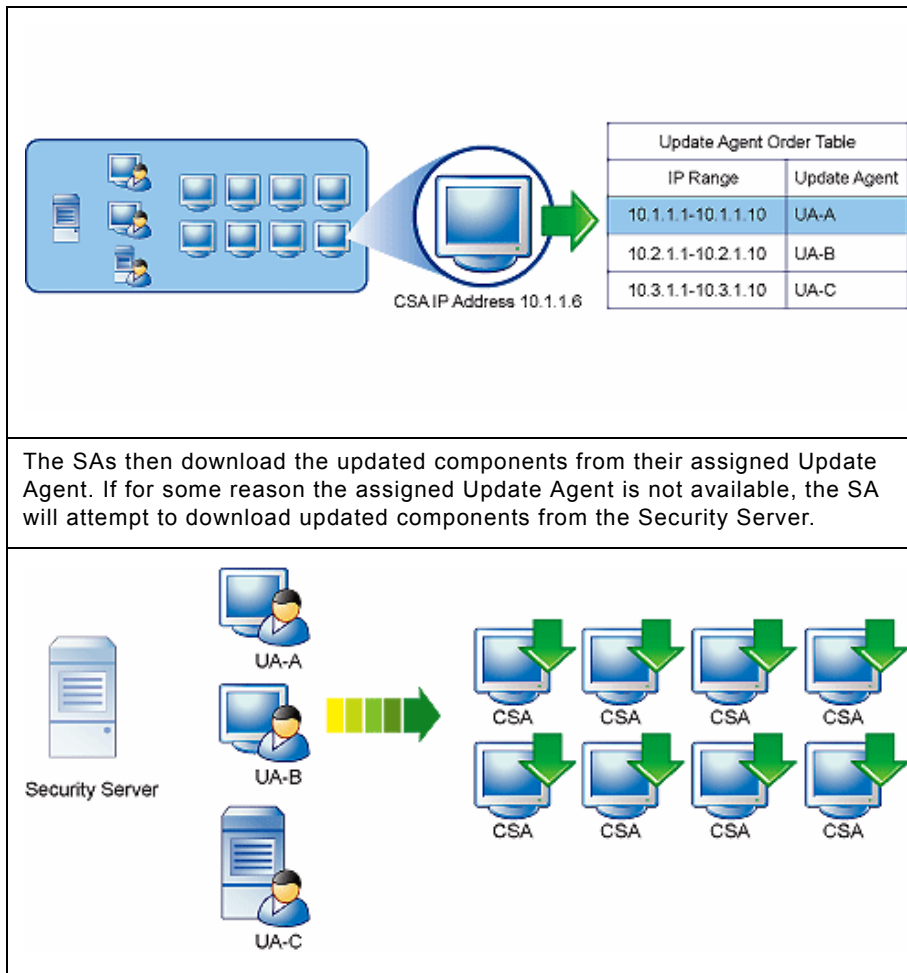
TABLE 7-2. Update Agents.

TABLE 7-2. Update Agents.

The Update Agent process works as follows:

Step 1. The Security Server notifies the Update Agents that new updates are available.

Step 2. The UAs download the updated components from the Security Server.

- Step 3.** The Security Server then notifies the Security Agents (SA) that updated components are available.
- Step 4.** Each SA loads a copy of the Update Agent Order Table to determine its appropriate update source. The order of the Update Agents in the Update Agent Order Table is initially determined by the order in which they were added as Alternative Update Sources. Each SA will go through the table one entry at a time, starting with the first entry, until it identifies its update source.
- Step 5.** The SAs then download the updated components from their assigned Update Agent. If for some reason the assigned Update Agent is not available, the SA will attempt to download updated components from the Security Server.

Using Update Agents

Navigation Path: Updates > Source > Add an Update Agent {tab}

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

Tip: If your network is segmented by location, Trend Micro recommends allowing at least one Agent on each segment to act as an Update Agent.

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 Agent on each segment to act as an Update Agent.

To allow Agents to act as Update Agents:

1. From the **Update Agents** tab on the **Source** screen, click **Add** in the **Assign Update Agents** section.
2. In the communication port input box, add the communication port for update Agents. The default port is the Security Agent's communication port + 1. Once this port is set, the input box will no longer appear.

Note: Do not confuse the Security Agent's port with the Update Agent port.

- The Security Agent port is used for communication between the Security Agent and the WFBS sever.
- The Update Agent port is used for communication between the Update Agent and other (non-Update-Agent) clients.

3. From the **Select Security Agents** list box, select one or more Agents to act as Update Agents.
4. Click **Save**.
To remove an Update Agent, select the check box corresponding to the **Computer Name** and click **Remove**.

Note: Unless specified in the Alternative Update Source section, all Update Agents receive their updates from the Trend Micro Security Server.

To allow Agents to get their updates from an alternative update source:

1. From the **Update Agents** tab on the **Source** screen, update the following options as required:
 - Enable Alternative Update Sources

- **Always update from Security Server for Update Agents:** This is an optional step to ensure Update Agents receive their updates only from the Security Server.

Note: If this option is selected, the Update Agents will download updates from the Trend Micro Security Server even if their IP address falls within one of the ranges specified in the **Add an Alternative Update Source** screen. For this option to work, **Enable Alternative Update Sources** must be selected.

2. Click **Save**.

To delete Update Agents:

1. From the main navigation menu select **Updates > Source**. The Updates Source screen appears.
2. Click the **Update Agents** tab.
3. Under the Assign Update Agent(s) heading, select the check box next to the Update Agent(s) that you wish to delete.
4. Click **Remove**. A message prompt appears asking you to confirm the deletion of the Update Agent(s). If you choose **OK**, the Update Agents will be deleted.

Manually Updating Components

Navigation Path: Updates > Manual

When you click **Update Now**, the Security Server searches for updated components. If updated components are available, the Security Server downloads them and starts deploying them to clients.

The Manual Update screen contains the following items:

- **Components:** Selects or clears all items on the screen.
- **Current Version:** Displays the current version of the component. Not necessarily the most recent version.
- **Last Update:** Displays the last time the Security Server downloaded the component.

☐	Components	Current Version	Last Update
 ☐	Messaging Security Agent Security Components		
 ☒	Smart Scan Pattern		
 ☒	AntiVirus and Anti-spyware		
 ☐	Outbreak Defense		
 ☐	Web Reputation		
 ☐	Behavior Monitoring and Device Control		
 ☐	Network Virus		
 ☐	Smart Protection Network		
☒	Security Components for Worry-Free Business Security Agent		

FIGURE 7-2. Manual Update Screen**To manually update components:**

- From the **Manual Update** screen, update the following options as required:
 - Components:** To select all components, select the Components check box. To select individual components, click  to display components and select the corresponding check boxes. For information about each component, see [Updatable Components](#) on page 7-18.
- Click **Update Now**.

Note: After the server downloads the updated components, it then automatically deploys the components to Agents.

Scheduling Component Updates

Navigation Path: Updates > Scheduled

By default the Scheduled screen contains the following items:

- Components tab:** Select components you want the Security Server to update.
 - Components:** Selects or deselects all items on the screen.
 - Current Version:** Displays the current version of the component. Not necessarily the most recent version.

- **Last Update:** Displays the last time the Security Server downloaded the component.

See *Updatable Components* on page 7-18 for information about each component.

- **Schedule tab:** Set the schedule that the Security Server uses to check for updated components.
 - **Daily:** Performs a scheduled scan every day.
 - **Weekly, every:** Performs a scheduled scan once a week. Select a day from the list.
 - **Monthly, on day:** Performs a scheduled scan once a month. Select a date from the list.

Regardless if you click Daily, Weekly, or Monthly, you must specify when to perform a scheduled scan in the Start time list boxes.

- **Save:** Click Save to ensure that your scheduled update settings are saved.

Schedule updates to automatically receive the latest components.

Tip: Avoid scheduling a scan and an update to run at the same time. This may cause the Scheduled Scan to stop unexpectedly.

Updates > Scheduled Update

Components Schedule

☒ Hourly
☐ Daily
☐ Weekly, every Sunday
☐ Monthly, on day 1

Start time: 12:00 (hh:mm) update for period of 2 hour(s)

Save

FIGURE 7-3. Scheduled Update screen

To schedule an update:

1. On the **Components** tab, select the components that you want to update. To select all components, select the check box next to **Components**.
2. On the **Scheduled** tab, choose how often to update the components.
3. Click **Save**.

Tip: During times of virus/malware outbreaks, Trend Micro responds quickly to update virus pattern files (updates can be issued more than once each week). The scan engine and other components are also updated regularly. Trend Micro recommends updating your components daily, or even more frequently in times of virus/malware outbreaks, to help ensure the Agent has the most up-to-date components.

Updatable Components

The ActiveUpdate server provides updated components such as virus pattern files, scan engines, and program files. After the server downloads any available updates, it automatically deploys the updated components to the Agents..

TABLE 7-3. Updatable Components

COMPONENT	SUB-COMPONENT
Messaging Security Agent (Advanced only)	Messaging Security Agent Anti-spam pattern Messaging Security Agent Anti-spam engine 32/64-bit Messaging Security Agent scan engine 32/64-bit Messaging Security Agent URL Filtering Engine 32/64-bit Messaging Security Agent pattern Messaging Security Agent Spyware active monitoring pattern Messaging Security Agent IntelliTrap exception pattern Messaging Security Agent IntelliTrap pattern

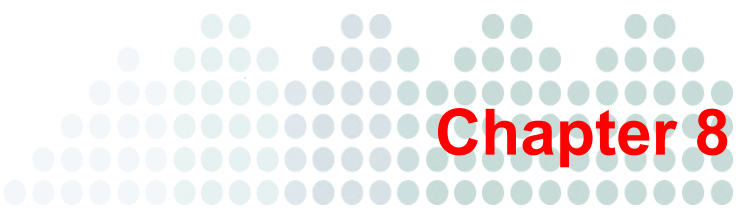
TABLE 7-3. Updatable Components (Continued)

COMPONENT	SUB-COMPONENT
Tools	CR pattern for Trend Micro Toolbar Trend Micro Toolbar Plug-in 32/64-bit Wi-Fi Plug-in 32/64-bit TMAS Plug-in 32/64-bit Rule based spam pattern
AntiVirus and Anti-spyware	IntelliTrap Pattern IntelliTrap Exception Pattern Spyware/Grayware Pattern v.6 Virus Pattern Damage Cleanup Template Spyware/Grayware Pattern Virus Scan Engine 32/64-bit System Event Monitoring Library 32/64-bit Spyware/Grayware Scan Engine v.6 32/64-bit Damage Cleanup Engine 32/64-bit
Outbreak Defense	Vulnerability Assessment Pattern 32/64-bit
Web Reputation	Web Page Analysis Rules URL Filtering Engine 32/64-bit
Behavior Monitoring and Device Control	Digital Signature Pattern Behavior Monitoring Configuration Pattern Behavior Monitoring Core Driver 32/64-bit Program Verification Library 32/64-bit Behavior Monitoring Core Library 32/64-bit System Event Monitoring Library 32/64-bit

TABLE 7-3. Updatable Components (Continued)

COMPONENT	SUB-COMPONENT
Network Virus	Firewall Pattern Firewall Service 32/64-bit TDI Driver 32/64-bit Firewall Driver - Windows Vista/7, 32/64-bit Firewall Driver - Windows XP, 32/64-bit
Smart Protection Network	Smart Feedback Engine 32/64-bit
Security Agent	Trend Micro Solution Platform - Framework Builder 32/64-bit Trend Micro Client Server Communicator 32/64-bit Security Agent Components 32/64-bit

See *Defense Components* on page 1-6 for detailed information about each component.



Chapter 8

Managing Notifications

This chapter explains how to use the different notification options.

The topics discussed in this chapter include:

- *Notifications* on page 8-2
- *Configuring Events for Notifications* on page 8-3
- *Customizing Notification Email Messages* on page 8-6
- *Configuring Notification Settings for Microsoft Exchange Servers (Advanced only)* on page 8-7

Notifications

Navigation Path: Preferences > Notifications

Administrators can receive notifications whenever there are abnormal events on the network. WFBS can send notifications using email, SNMP, or Windows event logs.

By default, all events listed in the Notifications screen are selected and trigger the Security Server to send notifications to the system Administrator.

Threat Events

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

System Events

- **Smart Scan:** Clients configured for Smart Scan cannot connect to the Smart Scan server or the server is not available.
- **Component update:** Last time components updated exceeds a certain number of days or updated components not deployed to Agents quick enough.
- **Unusual system events:** Remaining disk space on any of the clients running Windows Server operating system is less than the configured amount, reaching dangerously low levels.

License Events

- **License:** Product license is about to expire or has expired, seat count usage is more than 100%, or seat count is usage more than 120%.

Configuring Events for Notifications

Navigation Path: Preferences > Notifications

Configuring Notifications involves two steps. First, select the events for which you need notifications and then configure the methods of delivery. WFBS offers three methods for delivery: email notifications, SNMP notifications, and Windows Event log.

Email notifications are set on the Events tab; SNMP notifications and Windows Event logs are set on the Settings tab.

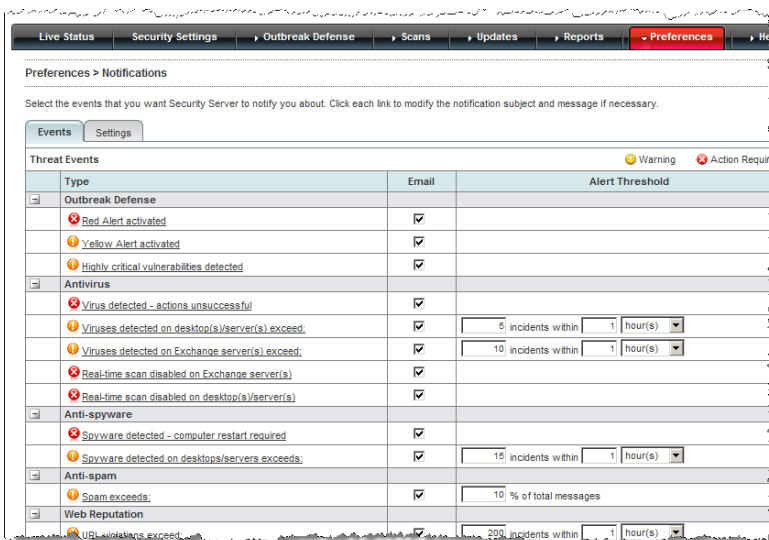


FIGURE 8-1. Notification Events screen

To configure notification events:

- From the **Events** tab on the **Notifications** screen, update the following as required:
 - Email:** Select the check box to receive a notifications for that event.
 - Alert Threshold:** Configure the threshold and/or time period for the event.
- Click **Save**.

Preferences > Notifications

Select the events that you want Security Server to notify you about. Click each link to modify the notification subject and message if necessary.

Events **Settings**

Email Notification

From: Administrator@TrendMicroWFBS.Local

To:

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

SNMP Notification Recipient

☐ Enable SNMP notifications ⓘ

IP Address:

Community:

Logging

☐ Write to Windows event log

FIGURE 8-2. Notifications Settings screen

To configure the notification delivery method:

1. From the **Settings** tab on the **Notifications** screen, update the following as required:
 - **Email Notification:** Set the email addresses of the sender and recipients.
 - **From**
 - **To:** Separate multiple email addresses with semicolons (;).
 - **SNMP Notification Recipient:** SNMP is protocol used by network hosts to exchange information used in the management of networks. To view data in the SNMP trap, use a Management Information Base browser.
 - **Enable SNMP notifications**
 - **IP Address:** The SNMP trap's IP address.
 - **Community:** The SNMP Community string
 - **Logging:** Notifications using the Windows Event log
 - **Write to Windows event log**
2. Click **Save**.

Customizing Notification Email Messages

Navigation Path: Preferences > Notifications > {Event}

Customize the subject line and the message body of event notifications.

To prevent email from addresses with external domains from being labeled as spam, add the external email addresses to the Approved Senders lists for Anti-Spam.

Tokens

Use the following tokens to represent threat events detected on desktops/servers and Exchange servers. The tokens refer to your selections on the **Preferences > Notifications > Events > Edit**.

- **{SCSM_SERVERNAME}** The name of the Security Server or Exchange server that detected the threat.
- **%CV** Number of incidents
- **%CU** The time unit (minutes, hours)
- **%CT** Number of %CU
- **%CP** Percentage of total email messages that is spam

The following is an example notification:

```
Trend Micro detected %CV virus incidents on your computer(s)
in %CT %CU. Virus incidents that are too numerous or too
frequent might indicate a pending outbreak situation.
```

Refer to the Live Status screen on the Security Server for further instructions.

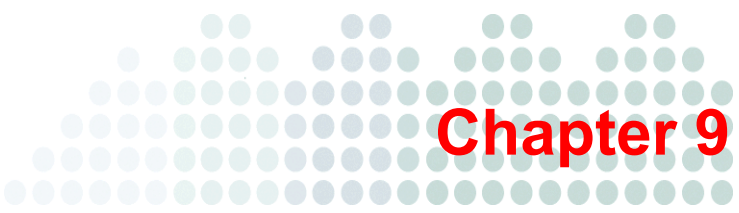
Configuring Notification Settings for Microsoft Exchange Servers (Advanced only)

Navigation Path: Security Settings > {MSA} > Configure > Operations > Notification Settings

Configure the Administrator address for notifications and define internal mails.

To configure notification settings:

1. From the Notification Settings screen, update the following as required:
 - **Email address:** The email address of the Worry-Free Business Security Administrator.
 - **Internal Email Definition**
 - **Default:** Worry-Free Business Security will treat email messages from the same domain Internal Emails.
 - **Custom:** Specify individual email addresses or domains to treat as internal email messages.
2. Click **Save**.



Chapter 9

Managing the Messaging Security Agent (Advanced only)

This chapter describes the Messaging Security Agent (MSA) and explains how to set Real-time Scan options, configure anti-spam, content filtering, attachment blocking, and quarantine maintenance options for Microsoft Exchange servers. Topics discussed in this chapter include:

- *Messaging Security Agents* on page 9-3
- *Antivirus* on page 9-12
- *Anti-Spam* on page 9-23
- *Content Scanning* on page 9-30
- *Content Filtering* on page 9-39
- *Data Loss Prevention* on page 9-65
- *Attachment Blocking* on page 9-87
- *Real-time Monitor* on page 9-90
- *Web Reputation* on page 9-91
- *Messaging Agent Quarantine* on page 9-93
- *Operations* on page 9-102

(TOC continued on next page)

- *Replicating Settings for Microsoft Exchange Servers* on page 9-108
- *Adding a Disclaimer to Outbound Email Messages* on page 9-108
- *Configuring Exclusions for Messaging Security Agents* on page 9-109
- *Advanced Scan Options for Microsoft Exchange Servers* on page 9-111
- *Advanced Macro Scanning* on page 9-112
- *Internal Address Definition* on page 9-113

Messaging Security Agents

Messaging Security Agents (MSAs) protect Microsoft Exchange servers. The MSA helps prevent email-borne threats by scanning email passing in and out of the Microsoft Exchange Mailbox Store as well as email that passes between the Microsoft Exchange Server and external destinations. In addition, the Messaging Security Agent can:

- reduce spam
- block email messages based on content
- block or restrict email messages with attachments
- detect malicious URLs in email
- prevent confidential data leaks

Messaging Security Agents can only be installed on Microsoft Exchange servers. The Tree displays all the Messaging Security Agents in a network.

Note: Multiple Messaging Security Agents cannot be combined into a Group. Administer and manage each Messaging Security Agent individually.

WFBS uses the Messaging Security Agent to gather security information from Microsoft Exchange servers. For example, the Messaging Security Agent reports spam detections or completion of component updates to the Trend Micro Security Server. This information displays in the Web Console. The Trend Micro Security Server also uses this information to generate logs and reports about the security status of your Microsoft Exchange servers.

Note: Each detected threat generates one log entry/notification. This means that if the Messaging Security Agent detects multiple threats in a single email, it will generate multiple log entries and notifications. There may also be instances when the same threat is detected several times, especially if you are using cache mode in Outlook 2003. When cache mode is enabled, the same threat may be detected both in the transport queue folder and Sent Items folder, or in the Outbox folder.

How the Messaging Security Agent Scans Email Messages

The Messaging Security Agent (MSA) uses the following sequence to scan email messages:

1. Scans for spam (Anti-spam)
 - a. Compares the email to the Administrator's Approved/Blocked Senders list
 - b. Checks for phishing occurrences
 - c. Compares the email with the Trend Micro supplied exception list
 - d. Compares the email with the Spam signature database
 - e. Applies heuristic scanning rules
2. Scans for content filtering rule violations
3. Scans for attachments that exceed user defined parameters
4. Scans for virus/malware (Antivirus)
5. Scans for malicious URLs

Messaging Security Agent Actions

Administrators can configure the Messaging Security Agent to take actions according to the type of threat presented by virus/malware, Trojans, and worms. If you use customized actions, set an action for each type of threat.

TABLE 9-1. Messaging Security Agent Customized Actions

ACTION	DESCRIPTION
Clean	Removes malicious code from infected message bodies and attachments. The remaining email message text, any uninfected files, and the cleaned files are delivered to the intended recipients. Trend Micro recommends you use the default scan action <i>clean</i> for virus/malware. Under some conditions, the Messaging Security Agent cannot clean a file. During a manual or Scheduled Scan, the Messaging Security Agent updates the Information Store and replaces the file with the cleaned one.
Replace with text/file	The Messaging Security Agent deletes the infected content and replaces it with text or a 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.
Quarantine entire message	Moves the email message to a restricted access folder, removing it as a security risk to the Microsoft Exchange environment. The original recipient will not receive the message. This option is not available in Manual and Scheduled Scanning. See Configuring Quarantine Directories on page 9-94 for more information about the quarantine folder.

TABLE 9-1. Messaging Security Agent Customized Actions (Continued)

ACTION	DESCRIPTION
Quarantine message part	Quarantines only the infected content to the quarantine directory and the recipient receives the message without this content.
Delete entire message	During Real-time Scanning, the Messaging Security Agent deletes the entire email message. The original recipient will not receive the message. This option is not available in Manual or Scheduled Scanning.
Pass	Records virus infection of malicious files in the Virus logs, but takes no action. Excluded, encrypted, or password-protected files are delivered to the recipient without updating the logs.
Archive	Moves the message to the archive directory and delivers the message to the original recipient.
Quarantine message to server-side spam folder	The Messaging Security Agent sends the entire message to the Security Server for quarantine.
Quarantine message to user's spam folder	The Messaging Security Agent sends the entire message to the user's spam folder for quarantine.
Tag and deliver	The Messaging Security Agent adds a tag to the header information of the email message that identifies it as spam and then delivers it to the intended recipient.

Configuring Scan Options for Microsoft Exchange Servers

Navigation Path: **Scans** > {Manual Scan or Scheduled Scan} > {MSA} > **Antivirus/Content Filtering/Attachment Blocking**

Configuring Scan Options for Microsoft Exchange servers involves setting options for Antivirus, Content Filtering, Attachment Blocking and Web Reputation.

To set the scan options for Microsoft Exchange Servers:

1. From the **Manual Scan** or **Scheduled Scan** screen, expand the Microsoft Exchange server to scan.
2. Set the scanning options for:
 - **Antivirus:** See *Configuring Manual or Scheduled Scans for Exchange Servers* on page 9-20
 - **Content Filtering:** See *Creating Content Filtering Rules* on page 9-43
 - **Attachment Blocking:** See *Configuring Attachment Blocking* on page 9-89
 - **Web Reputation:** See *Web Reputation* on page 9-91
3. For Scheduled Scans, update the schedule on the **Schedule** tab. See *Scheduling Scans* on page 6-9.
4. Click **Scan Now** or **Save**.

Default Messaging Security Agent Settings

Consider the options listed in the table to help you optimize your Messaging Security Agent configurations.

TABLE 9-2. Trend Micro Default Actions for the Messaging Security Agent

SCAN OPTION	REAL-TIME SCAN	MANUAL AND SCHEDULED SCAN
Anti-spam		
Spam	Quarantine message to user's spam folder (default, if the Outlook Junk Email or End User Quarantine installed)	Not applicable

TABLE 9-2. Trend Micro Default Actions for the Messaging Security Agent

SCAN OPTION	REAL-TIME SCAN	MANUAL AND SCHEDULED SCAN
Phish	Delete entire message	Not applicable
Content filtering		
Filter messages that match any condition defined	Quarantine entire message	Replace
Filter messages that match all conditions defined	Quarantine entire message	Not available
Monitor the message content of particular email accounts	Quarantine entire message	Replace
Create an exception for particular email accounts	Pass	Pass
Attachment blocking		
Action	Replace attachment with text/file	Replace attachment with text/file
Other		
Encrypted and Password protected files	Pass (When you configure the action to Pass, encrypted files and files that are protected by passwords are passed and the event is not logged)	Pass (When you configure the action to Pass, encrypted files and files that are protected by passwords are passed and the event is not logged)

TABLE 9-2. Trend Micro Default Actions for the Messaging Security Agent

SCAN OPTION	REAL-TIME SCAN	MANUAL AND SCHEDULED SCAN
Excluded files (Files over specified scanning restrictions)	Pass (When you configure the action to Pass, files or message body over the specified scanning restrictions are passed and the event is not logged)	Pass (When you configure the action to Pass, files or message body over the specified scanning restrictions are passed and the event is not logged)

Installing MSAs to Microsoft Exchange Servers

When you Add a Microsoft Exchange server, the Security Server deploys the MSA to the Microsoft Exchange server and adds the icon for that Exchange server to the Security Groups Tree. The client Microsoft Exchange server is added to your list of computers on the **Security Settings** screen. Once the MSA is installed to your client, it will start to report security information to the Security Server.

You can install the Messaging Security Agent using two methods:

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

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

When installing the Security Server on a computer that has Microsoft Exchange server installed on the same computer, Setup prompts you to do a local install of the Messaging Security Agent (This is true only if you chose the Messaging Security Agent on the Select Components page of the installer).

Note: Worry-Free Business Security will automatically detect the Microsoft Exchange server name and automatically fill in the Exchange Server Name field. If you have an Exchange Server installed on same machine, but the Exchange Server Name is not automatically filled in, check if the environment meet MSA system requirements.

When installing the Security Server on a computer that has remote Microsoft Exchange servers connected to the same network, Setup prompts you to install the Messaging Security Agent to remote servers (This is true only if you chose the Messaging Security Agent on the Select Components page of the installer. However, if there is an Exchange Server on the computer to which you are installing the Security Server, the Remote Messaging Agent will not show on the Select Components page; only the local Messaging Security Agent will show). See the Administrator's Guide for instructions about installing to a local Microsoft Exchange server.

- **Method 2:** Install the Messaging Security Agent from the Web Console after installation is complete. You can install to one or more remote Microsoft Exchange servers using this method.

To add a Desktop or Microsoft Exchange Server:

1. Open the **Security Settings** screen.
2. Click **Add**. The **Security Settings > Add Computer** screen opens.
3. Select Exchange server. The screen changes to display the Server name, Account, and Password. Type your information here. The Account must be a Domain Administrator account.
4. Click **Next**. The installation wizard displays a screen depending on the type of installation you need to do.
 - **Fresh installation:** Installing to a Microsoft Exchange server with no previous versions of Messaging Security
 - **Upgrade:** Installing to a Microsoft Exchange server which has a previous version of Messaging Security (otherwise known as ScanMail)
 - **No installation required:** Add a Microsoft Exchange server that already has Messaging Security installed to the Security Groups Tree
 - **Invalid:** A message warns you that there is a problem with your installation.

Removing Microsoft Exchange Servers from the Web Console

Navigation Path: Security Settings > {MSA} > Remove

You can use Remove to accomplish two goals:

- **Remove** the Client icon from the Web Console
In some situations, the Microsoft Exchange Server might become inactive such as when the computer has been reformatted or the administrator disables the Messaging Security Agent for a long time. In these situations, you might want to delete the computer icon from the Web Console.
- **Uninstall** the Messaging Security Agent from the Microsoft Exchange server (and consequently remove the Client icon from the Web Console)

As long as a Microsoft Exchange server has the MSA installed, it is capable of becoming active and appearing on the Web Console. To remove the inactive Microsoft Exchange server for good, first uninstall the MSA.

Note: Note: If you have Microsoft Exchange 5.5 Servers running ScanMail 3.82 connected to your network, you cannot uninstall from the Web Console.

You can remove either a single Microsoft Exchange server or a group from the Web Console.

WARNING! Removing the MSA from a computer may expose the Microsoft Exchange server to viruses and other malware.

To remove a Microsoft Exchange server:

1. Click the Microsoft Exchange server or group that you want to remove from the Web Console.
2. Click **Remove** from the toolbar.
 - a. Select **Remove** to remove the client icon from the Web Console.

- b. Select **Uninstall** to remove the MSA from the selected Microsoft Exchange server and remove the computer icons from the Web Console.
 - i. If necessary, type the account name and password for the Microsoft Exchange server that you want to remove.
 - ii. Click **OK** from the warning message to complete the uninstallation.
3. Click **Next**.
4. Confirm your action by clicking **Apply**.

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

Antivirus

WFSB provides three types of scans to protect Microsoft Exchange Servers from email-borne threats:

- **Real-time Scan:** Real-time Scan is a persistent and ongoing scan. The Messaging Security Agent (MSA) guards all known virus entry points with Real-time Scanning of all incoming messages, SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers. When it detects a security threat it automatically takes action against those security risks according to the configurations.

The Messaging Security Agent scans the following in real time:

- All incoming and outgoing email messages
- Public-folder postings
- All server-to-server replications

The speed of Real-time Scanning depends on its settings. You can increase the performance of Real-time Scans by specifying certain file types that are vulnerable to virus/malware.

- **Manual Scan:** Manual Scan is an on-demand scan. Manual Scanning eliminates threats from files on clients and inside Microsoft Exchange mailboxes. This scan also eradicates old infections, if any, to minimize reinfection. During a Manual Scan, WFBS takes actions against threats according to the actions set by the Administrator.

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

Configuring Real-Time Scans for Exchange Servers

Navigation Path: Security Settings > {MSA} > Configure > Antivirus

By default, the Messaging Security Agent has Real-time scanning enabled and uses Trend Micro recommended settings when running scans. When the MSA detects a security threat it automatically takes action against those threats according to these settings and logs the actions. Trend Micro designed these settings to provide optimal protection for small and medium-sized businesses. No post-installation configuration is necessary to protect your Microsoft Exchange servers. However, if desired, you can customize your scan options for Real-time scans, Manual scans, and Scheduled scans. See Table 9-2 on page 9-7 for default settings.

Note: Real-time scan options are very similar to Manual scan options and Scheduled scan options. Set the options for Manual and Scheduled scans from **Scans > Manual** or **Scans > Scheduled**.

Antivirus

☒ Enable real-time antivirus

Target
Action

Default Scan

Select a method for scanning viruses, worms, Trojans, and other malicious code:

☒ All scannable files

☐ IntelliScan: uses "true file type" identification

☐ Specific file types

☒ Enable IntelliTrap

☒ Scan message body

Additional Threat Scan

☐ Select All

☒ Spyware

☐ Dialers

☐ Hacking Tools

☐ Password Cracking Applications

☒ Adware

☐ Joke Programs

☐ Remote Access Tools

☐ Others

Exclusions

Do not scan attachment and/or message body if:

☒ Message body size exceeds: 30 MB

☒ Attachment size exceeds: 30 MB

Do not scan compressed files if:

☒ Decompressed file count exceeds: 9999

☒ Size of decompressed file exceeds: 100 MB

☒ Number of layers of compression exceeds: 5 (1-20)

☒ Size of decompressed file is "x" times the size of compressed file: 1000 (1-1000000)

Save
Reset

FIGURE 9-1. Antivirus screen

Note: The Trend Micro default, **All scannable files**, provides the maximum security possible. However, scanning every message requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the MSA includes in the scan.

To configure Real-time Scan for Messaging Security Agents:

1. From the **Target** tab on the **Antivirus** screen, update the following as required:
 - Enable real-time antivirus
 - **Default Scan**
 - **Select a method**
 - **All attachment files**
 - **IntelliScan:** Scans files based on true-file type. See [IntelliScan](#) on page D-4.
 - **Specific file types:** WFBS will scan files with the selected extensions. Separate multiple entries with commas (,).
-
- Note:** The following file types are always .com, ASCII, TEXT, HTML, and Active Server pages.
-
- **Enable IntelliTrap:** IntelliTrap detects malicious code such as bots in compressed files. See [IntelliTrap](#) on page D-6.
 - **Scan message body:** Scans the body of an email message that could contain embedded threats.
 - **Additional Threat Scan:** Select the additional threats WFBS should scan. See [Understanding Threats](#) on page 1-10 for definitions of threats.
 - **Exclusions:** Exclude email messages that match the following criteria from scans:
 - Message body size exceeds
 - Attachment size exceeds
 - Decompressed file count exceeds
 - Size of decompressed file exceeds
 - Number of layers of compression exceeds
 - Size of decompressed file is “x” times the size of compressed file
 2. From the **Action** tab, update the following as required:
 - Action for Virus Detections
 - **ActiveAction:** Use Trend Micro preconfigured actions for threats. See [ActiveAction](#) on page D-4.

- **Customized Action**
 - **Perform the same action for all detected Internet threats:** Select from Clean, Replace with Text/File, Quarantine entire message, Delete entire message, Pass, or Quarantine message part. See Table 9-1 on page 9-5.
 - **Specify action per detected threats:** Select from Clean, Replace with text/file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part for each type of threat. See Table 9-1 on page 9-5.
 - **Enable action on Mass-mailing behavior:** Select from Clean, Replace with text/file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part for mass-mailing behavior type of threats. See Table 9-1 on page 9-5.
- **Do this when clean is unsuccessful:** Set the secondary action for unsuccessful cleaning attempts. Select from Replace with Text/File, Quarantine entire message, Delete entire message, Pass, or Quarantine message part.
- **Backup infected file before performing action:** Back up the threat before cleaning as a precaution to protect the original file from damage.

Note: Trend Micro recommends deleting backed up files immediately after determining the original file was not damaged and that it is usable. If the file becomes damaged or unusable, send it to Trend Micro for further analysis. (Even if the Messaging Security Agent has completely cleaned and removed the virus itself, some virus/malware damage the original file code beyond repair.)

- **Do not clean infected compressed files to optimize performance:** When Agents detect a threat in a compressed file, it will not clean the file. Instead, it processes the files as if they were uncleanable.
- **Notification:** WFBS will send notification messages to the selected people. Administrators can also disable sending notifications to spoofing senders.
- **Macros:** A type of virus encoded in an application macro and often included in a document. Select **Enable advanced macro scan** and configure the following:

- **Heuristic level:** Heuristic scanning is an evaluative method of detecting viruses. This method excels at detecting undiscovered viruses and threats that do not have a known virus signature.
- **Delete all macros detected by advanced macro scan:** See [Advanced Macro Scanning](#) on page 9-112.
- **Unscannable Message Parts:** Set the action and notification condition for encrypted and/or password-protected files. For the action, select from Replace with text/file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part.
- **Excluded Message Parts:** Set the action and notification condition for parts of messages that have been excluded. For the action, select from Replace with text/file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part.
- **Backup Setting:** The location to save the backed up files.
- **Replacement Settings:** Configure the text and file for replacement text. If the action is replace with text/file, WFBS will replace the threat with this text string and file.

3. Click **Save**.

To configure who receives notifications when an event occurs, see [Configuring Events for Notifications](#) on page 8-3.

Manual Scans for Microsoft Exchange Servers

Navigation Path: Scans > Manual Scan > {MSA} > Antivirus

When the MSA runs a Manual scan, it scans all the files in the Information Store of your Microsoft Exchange server. Manual Scans start immediately after you click **Scan Now** and runs until the MSA has scanned all the specified files or you interrupt the scan by clicking Stop Scanning. The length of the scan depends on the number of files you specified for scanning and your hardware resources. Trend Micro recommends running Manual scans after a virus outbreak.

The MSA has Real-time scanning enabled by default. Run Manual scans to supplement Real-time scanning protection or to detect specific virus or malware threats.

By default, the MSA uses Trend Micro recommended settings when running Manual scans. When the MSA detects a security threat it automatically takes action against those threats according to these settings and logs the actions. You can view the results on the Live Status screen or by generating reports or log queries.

To run a manual scan:

1. Click **Scans > Manual Scan**. Accept the Trend Micro recommended default settings or customize your scan.
2. Select the item(s) to scan.
3. Click **Scan Now**. The Scan Notifying Progress screen appears. When the scan notification is complete the Scan Notifying Results screen appears to show you the results of the scan notifications.

Default Manual Scan settings recommended by Trend Micro:

- The MSA scans All scannable files. It includes the message bodies of email messages in the scan.
- When the MSA detects a file with a virus or other malware, it cleans the file. When it cannot clean the file, it replaces with text/file instead.
- When the MSA detects a file with a Trojan or worm, it replaces the Trojan or worm with a text or file.
- When the MSA detects a file with a Packer, it replaces the Packer with a text or file.
- The MSA does not clean infected compressed files. This reduces the time required during real-time scanning.

Note: Trend Micro designed these settings to provide optimal protection for small and medium-sized businesses. When running Manual scans, no post-installation configuration is necessary to protect your Microsoft Exchange servers. However, if desired, you can customize your scan options.

Scheduled Scans for Microsoft Exchange Servers

Navigation Path: Scans > Scheduled Scan > {MSA} > Antivirus

A Scheduled scan is a Manual scan that runs according to a schedule. Scheduled scans can run on a daily, weekly, or monthly schedule. You can set the time when to begin the Scheduled scan. This allows you to run your Scheduled scan when network traffic is low.

Tip: Trend Micro recommends that you not schedule a scan at the same time as a scheduled update. This may cause the scheduled scan to stop unexpectedly. Similarly, if you begin a manual scan when a scheduled scan is running, the scheduled scan is interrupted. The scheduled scan aborts, but will run again according to its schedule.

The MSA has Real-time scanning enabled by default. Run Scheduled scans to supplement Real-time scanning protection.

By default, the MSA uses Trend Micro recommended settings when running scheduled scans. When it detects a security threat it automatically takes action against those threats according to these settings and logs the actions. You can view the results on the Live Status screen or by generating reports or log queries.

Trend Micro recommended default Scheduled Scan settings:

- The MSA performs a scan every Sunday, starting at 5:00 AM.
- Customize this schedule to run during an off-peak time for your Clients. The MSA scans All scannable files. It includes the message bodies of email messages in the scan.
- When the MSA detects a file with a virus or other malware, it cleans the file. When it cannot clean the file, it replaces with text/file instead.
- When the MSA detects a file with a Trojan or worm, it replaces the Trojan or worm with a text/file.
- When the MSA detects a file with a Packer, it replaces it with text/file.
- The MSA does not clean infected compressed files.

Configuring Manual or Scheduled Scans for Exchange Servers

Navigation Path: Scans > Manual Scan or Scheduled Scan > {MSA} > Antivirus

Customize your scans in two or three steps: first set the target files to scan and set exclusions, set the actions for the MSA to take against detected threats. If this is a scheduled scan, set the schedule.

Step 1. Set the target files and set exclusions, if any.

The Trend Micro default, **All scannable files**, provides the maximum security possible. However, scanning every message requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the MSA includes in the scan.

Step 2. Set the actions for the MSA to take against detected threats.

When the MSA detects a file that matches your scanning configurations, it executes an action to protect your Microsoft Exchange environment. The type of action it executes depends on the type of scan it is performing (real-time, manual, or scheduled) and the type of actions you have configured for that scan.

Step 3. Set the schedule for when the scan will take place.

To set the antivirus scan options for Microsoft Exchange Servers:

1. From the Antivirus screen, update the options as required:

- **Default Scan**

- **All scannable files:** Only encrypted or password-protected files are excluded.
- **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.
- **Specific File Types:** Worry-Free Business Security Advanced will scan files of the selected types and with the selected extensions. Separate multiple entries with semicolons(;).

- **Enable IntelliTrap:** IntelliTrap detects malicious code such as bots in compressed files.
- **Scan message body:** Scans the body of an email message that could contain embedded threats.
- **Additional Threat Scan:** Select the additional threats Worry-Free Business Security Advanced should scan.
- **Exclusions:** Exclude email messages that match the following criteria from scans:
 - **Message body size exceeds**
 - **Attachment size exceeds**
 - **Decompressed file count exceeds**
 - **Size of decompressed file exceeds**
 - **Number of layers of compression exceeds**
 - **Size of decompressed file is "r;x" times the size of compressed file**

2. From the Action tab, update the following as required:

- Action for Virus Detections
 - **ActiveAction:** Use Trend Micro preconfigured actions for threats. See [ActiveAction](#) on page D-4.
 - **Same action for all threats:** Select from Clean, Replace with Text/File, Delete Entire message, Pass, or Quarantine the message part.
 - **Customized action for the following detected threats:** Select from Clean, Replace with Text/File, Delete Entire message, Pass, or Quarantine message part for each type of threat.
 - **Enable action on Mass-mailing behavior:** Select from Clean, Replace with Text/File, Delete Entire message, Pass, or Quarantine message part for mass-mailing behavior type of threats. Set the secondary action for unsuccessful cleaning attempts. Select from Replace with Text/File, Delete Entire message, Pass, or Quarantine the message part.

- **Backup infected file before cleaning:** Worry-Free Business Security Advanced makes a backup of the threat before cleaning. The backed-up file is encrypted and stored in the following directory on the client:
C:\Program Files\Trend Micro\Messaging Security Agent\Backup
To decrypt the file, see [Restoring an Encrypted Virus](#) on page B-12
- **Do not clean infected compressed files to optimize performance**
- **Notifications:** Worry-Free Business Security Advanced will send notification messages to the selected people. Administrators can also disable sending notifications to spoofing senders external recipients.
- **Macros:** Macro viruses are application-specific viruses that infect macro utilities that accompany applications.
- **Heuristic level:** Heuristic scanning is an evaluative method of detecting viruses. This method excels at detecting undiscovered viruses and threats that do not have a known virus signature.
- **Delete all macros detected by advanced macro scan:** See [Advanced Macro Scanning](#) on page 9-112.
- **Unscannable Message Parts:** Set the action and notification condition for encrypted and/or password-protected files. For the action, select from Replace with Text/File, Delete Entire message, Pass, or Quarantine message part.
- **Excluded Message Parts:** Set the action and notification condition for parts of messages that have been excluded. For the action, select from Replace with Text/File, Delete Entire message, Pass, or Quarantine message part.
- **Backup Setting:** The location to save the backed up files.
- **Replacement Settings:** Configure the text and file for replacement text. If the action is replace with text/file, Worry-Free Business Security Advanced will replace the threat with this text string and file.

3. Click **Save**.

To set Scheduled Scan settings:

Navigation Path: Scans > Scheduled Scan > {MSA} > Antivirus

1. Click the **Settings** tab.
2. Select the Microsoft Exchange servers for which you want to set the scheduled scan.

3. Click the **Schedule** tab to specify when to perform scheduled scan.
 - **Daily**
 - **Weekly, every:** perform a scheduled scan once a week, then select a day from the list
 - **Monthly, on day:** perform a scheduled scan once a month, then select a date from the list
 - Whether you click **Daily**, **Weekly**, or **Monthly**, you must specify when to perform a scheduled scan in the Start time list boxes.
4. If necessary, set scan options.
5. Click **Save**.

Additionally, configure who receives notifications when an event occurs. See [Notification Settings](#) on page 9-103.

Anti-Spam

Email Reputation technology determines spam based on the reputation of the originating Mail Transport Agent (MTA). This off-loads the task from the Worry-Free Business Security Advanced server. With Email Reputation enabled, all inbound SMTP traffic is checked by the IP databases to see whether the originating IP address is clean or it has been black-listed as a known spam vector.

WFBS provides two ways to combat spam—Email Reputation and Content Scanning.

The MSA uses the following components to filter email messages for spam and phishing incidents:

- Trend Micro Anti-Spam Engine
- Trend Micro spam pattern files

Trend Micro updates both the engine and pattern file frequently and makes them available for download. The Security Server can download these components through a manual or scheduled update.

The anti-spam engine uses spam signatures and heuristic rules to filter email messages. It scans email messages and assigns a spam score to each one based on how closely it matches the rules and patterns from the pattern file. The MSA compares the spam score to the user-defined spam detection level. When the spam score exceeds the detection level, the MSA takes action against the spam.

For example: Spammers often use many exclamation marks or more than one consecutive exclamation mark(!!!) in their email messages. When the MSA detects a message that uses exclamation marks this way, it increases the spam score for that email message.

Tip: In addition to using Anti-Spam to screen out spam, you can configure Content Filtering to filter message header, subject, body, and attachment information to filter out spam and other undesirable content.

Users cannot modify the method that the anti-spam engine uses to assign spam scores, but they can adjust the detection levels used by the MSA to decide what is spam and what is not spam.

Configuring Anti-Spam

Navigation Path: Security Settings > {MSA} > Configure > Anti-spam

The following are the basic steps to setting up spam screening:

1. Select **Enable Anti-Spam**.
2. Select the **Target** tab to select the method and spam detection rate that the Messaging Security Agent uses to screen for spam:
 - a. Select the detection level, **low**, **medium**, or **high**, from the spam detection rate list. The Messaging Security Agent uses this rate to screen all messages.
 - b. Add addresses to your list of Approved Senders and Blocked Senders.
 - c. Click Detect Phishing incidents to have the Messaging Security Agent screen out Phishing Incidents.
3. Select the **Action** tab to set the actions that the Messaging Security Agent takes when it detects a spam message or phishing incident.

The Messaging Security Agent detects spam message in real time and takes actions to protect the Microsoft Exchange Clients. The Messaging Security Agent takes one of the following actions depending on your configuration:

- **Quarantine message to server-side spam folder**

The Messaging Security Agent moves the message to the Spam Mail folder located on the server-side of the information store.

- **Quarantine message to user's spam folder**

The Messaging Security Agent moves the message to the user's Spam Mail folder located on the server-side of the Information Store.

- **Delete entire message**

The Messaging Security Agent deletes the entire message and Microsoft Exchange does not deliver it.

- **Tag and deliver**

The Messaging Security Agent adds a tag to the header information of the email message that identifies it as spam and then delivers it to the intended recipient.

4. Save your changes.

Spam Detection Settings

Navigation Path: Security Settings > {MSA} > Configure > Anti-spam

Use the Anti-spam screen to set the Messaging Security Agent to filter email messages to detect and screen out spam.

Recommended settings:

- Trend Micro recommends a Medium spam detection level

Use these features to screen messages for spam:

Spam Detection Rate:

Set a spam detection rate to screen out spam. The higher the detection level, the more messages classified as spam.

- **High:** This is the most rigorous level of spam detection. The Messaging Security Agent monitors all email messages for suspicious files or text, but there is greater chance of false positives. False positives are those email messages that the Messaging Security Agent filters as spam when they are actually legitimate email messages.
- **Medium:** This is the default setting. The Messaging Security Agent monitors at a high level of spam detection with a moderate chance of filtering false positives.
- **Low:** This is most lenient level of spam detection. The Messaging Security Agent will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives. Filtering by spam score.

Approved and Blocked sender lists:

The Messaging Security Agent always categorizes email messages from blocked senders as spam and takes the appropriate action. The Messaging Security Agent never categorizes email messages from approved senders as spam. The Messaging Security Agent delivers these messages to the original recipient without taking any anti-spam action.

Note: The Microsoft Exchange administrator maintains a separate Approved and Blocked Senders list for the Microsoft Exchange server. If an end-user creates an approved sender, but that sender is on the administrator's Blocked Senders list, then the Messaging Security Agent detects messages from that blocked sender as spam and takes action against those messages.

Managing End User Quarantine

The Spam Maintenance screen allows you to configure settings for the End User Quarantine (EUQ) or Server-side quarantine.

You configure the following features from this screen:

Enable End User Quarantine tool: When you enable the EUQ tool, a quarantine folder is created on the server-side of each Client's mailbox and a Spam Mail folder appears in the end user's Outlook folder tree. After EUQ is enabled and the Spam Mail folders are created, EUQ will filter spam mail to the user's Spam mail folder.

Tip: If you select this option, Trend Micro recommends disabling the Trend Micro Anti-Spam toolbar option on Agents to increase performance on Clients.

Note: You must enable the EUQ tool in order for the “Anti-spam > quarantine message to user's spam folder” action to work.

- **Create spam folder and delete spam messages:** Clicking this tool will create (immediately) Spam Mail folders for newly created mail clients and for existing mail clients that have deleted their Spam Mail folder. For other existing mail clients, it will delete spam messages that are older than the days specified in the Client Spam Folder Settings field.
- **Delete spam messages older than {number} days:** Modify the length of time that the Messaging Security Agent (MSA) will retain spam messages.
- **Add users who want to have End User Quarantine tool disabled:** Disables the End User Quarantine tool for each user you add to the User List Settings.
- **End User Quarantine tool for these users will be disabled:** Disables the End User Quarantine tool for each user you add to the User List Settings.

To disable the End User Quarantine Tool:

Clear **Enable End User Quarantine tool** to disable the end user quarantine tool for all mailboxes on your Microsoft Exchange server. When you disable the EUQ tool, the users' Spam Mail folders will remain, but messages detected as spam will not be moved to the Spam Mail folders.

To disable an individual end user's EUQ spam folder:

1. Under **End User Quarantine tool exception list**, type the email address of the end user for whom you want to disable EUQ.

2. Click **Add**. The end user's email address is added to the list of addresses that have EUQ disabled. To remove an end user from the list and restore EUQ service, select the end user's email address from the list and click Delete.
3. Click **Save**.

To create the spam mail folder:

1. Click **Create spam folder** and delete spam messages.
2. Click **Save**.

To reset the storage time limit:

1. Type the number of days you want MSA to retain the spam in the field next to Delete spam messages older than: (the default value is 14 days and the maximum time limit is 30 days).
2. Click **Save** to save your change and close the screen.

Email Reputation

Email Reputation technology determines spam based on the reputation of the originating Mail Transport Agent (MTA). This off-loads the task from the Worry-Free Business Security Server. With Email Reputation enabled, all inbound SMTP traffic is checked by the IP databases to see whether the originating IP address is clean or it has been black-listed as a known spam vector.

There are two service levels for Email Reputation. They are:

- **Standard:** The Standard service uses a database that tracks the reputation of about two billion IP addresses. IP addresses that have been consistently associated with the delivery of spam messages are added to the database and rarely removed.
- **Advanced:** The Advanced service level is a DNS, query-based service like the Standard service. At the core of this service is the standard reputation database, along with the dynamic reputation, real-time database that blocks messages from known and suspected sources of spam.

When an email message from a blocked or a suspected IP address is found, Email Reputation blocks the message before it reaches your gateway.

Configuring Email Reputation

Navigation Path: Security Settings > {MSA} > Configure > Anti-Spam > Email Reputation

Configure Email Reputation to block messages from known or suspected sources of spam. Additionally, create exclusions to allow or block message from other senders.

Anti-Spam (Email Reputation)

☒ Enable real-time anti-spam (Email Reputation)

Target Service Portal

Service Level

Set service level:

☐ Standard
Uses the Standard Reputation database to block messages from known spam sources. [Click for more information.](#)
Intelligent action - Denial of connection for standard reputation matches

☒ Advanced
Uses both Standard and Dynamic Reputation databases to block messages from known and suspected spam sources. [Click for more information.](#)
Intelligent action - Denial of connection for advanced reputation matches

Approved IP Addresses

Blocked IP Addresses

Save Restore Defaults

FIGURE 9-2. Email Reputation screen

To configure Email Reputation:

- From the **Target** tab on the **Email Reputation** screen, update the following as required:
 - Enable real-time Anti-Spam (Email Reputation)**
 - Service Level:**
 - Standard**
 - Advanced**
 - Approved IP Addresses:** Email messages from these IP addresses will never be blocked. Type the IP address to approve and click **Add**. If required, you can import a list of IP addresses from a text file. To remove an IP address, select the address and click **Remove**.

- **Blocked IP Addresses:** Email messages from these IP addresses will always be blocked. Type the IP address to block and click **Add**. If required, you can import a list of IP addresses from a text file. To remove an IP address, select the address and click **Remove**.
2. Click **Save**.
 3. Go to: <http://ers.trendmicro.com/> to view reports.
-

Note: Email Reputation is a Web-based service. Administrator's can only configure the service level from the Web Console.

Content Scanning

Content Scanning identifies spam based on the content of the message rather than the originating IP. The Messaging Security Agent uses the Trend Micro anti-spam engine and spam pattern files to screen each email message for spam before delivering it to the Information Store. The Microsoft Exchange server will not process rejected spam mail and the messages do not end up in the user's mailboxes.

Note: Do not confuse Content Scanning (anti-spam based on signatures and heuristics) with Content Filtering (email scanning and blocking based on categorized keywords). See [Content Filtering](#) on page 9-39

Spam Detection

The anti-spam engine makes use of spam signatures and heuristic rules to screen email messages. It scans email messages and assigns a spam score to each one based on how closely it matches the rules and patterns from the pattern file. The Messaging Security Agent compares the spam score to the user-defined spam detection level. When the spam score exceeds the detection level, the Messaging Security Agent takes action against the spam.

For example, spammers often use many exclamation marks, or more than one consecutive exclamation marks (!!!!) in their email messages. When the Messaging Security Agent detects a message that uses exclamation marks in this way, it increases the spam score for that email message.

Select one of these options for your spam detection:

- **High:** This is the most rigorous level of spam detection, but there is greater chance of false positives. False positives are those emails that the Messaging Security Agent filters as spam when they are actually legitimate emails.
- **Medium:** This is the default setting. The Messaging Security Agent monitors at a high level of spam detection with a moderate chance of filtering false positives.
- **Low:** This is most lenient level of spam detection. The Messaging Security Agent will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives.

The Messaging Security Agent performs one of the following actions on detected spam during Real-time Scanning:

- **Quarantine message to server-side spam folder**
- **Quarantine message to user's spam folder**
- **Delete entire message**
- **Tag and deliver:** The MSA adds a tag to the header information of the email message that identifies it as spam and then delivers it to the intended recipient.

Note: Microsoft Outlook may automatically filter and send messages that the MSA detected as spam to the Junk Mail folder.

Phishing

A Phishing incident starts with an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click a link that will redirect their browsers to a fraudulent website. Here the user is asked to update personal information such as passwords, social security numbers, and credit card numbers in an attempt to trick a recipient into providing private information that will be used for identity theft.

When the MSA detects a Phishing message, it can take the following actions:

- **Quarantine message to server-side spam folder**
- **Delete entire message**
- **Tag and deliver:** The adds a tag to the header information of the email message that identifies it as phish and then delivers it to the intended recipient.

Phishing Incidents

Phish Attack

Phish, or phishing, is a rapidly growing form of fraud that seeks to fool web users into divulging private information by mimicking a legitimate website.

In a typical scenario, unsuspecting users get an urgent sounding (and authentic looking) email telling them there is a problem with their account that they must immediately fix to avoid account termination. The email will include a URL to a website that looks exactly like the real thing. It is simple to copy a legitimate email and a legitimate website but then change the so-called backend, which receives the collected data.

The email tells the user to log on to the site and confirm some account information. A hacker receives data a user provides, such as a logon name, password, credit card number, or social security number.

Phish fraud is fast, cheap, and easy to perpetuate. It is also potentially quite lucrative for those criminals who practice it. Phish is hard for even computer-savvy users to detect. And it is hard for law enforcement to track down. Worse, it is almost impossible to prosecute.

Please report to Trend Micro any website you suspect to be a phishing site. See [Sending Suspicious Files to Trend Micro](#) on page I-5 for more information.

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.

Detecting and Removing Phishing Incidents

Navigation Path: Security Settings > {MSA} > Configure > Anti-spam

A Phish is an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click a link that will redirect their browsers to a fraudulent website where 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 will be used for identity theft.

When the Messaging Security Agent detects a Phish message, it can take the following actions:

- **Delete entire message**

The Messaging Security Agent deletes the entire message and Microsoft Exchange does not deliver it.

- **Tag and deliver**

The Messaging Security Agent adds a tag to the header information of the email message that identifies it as phish and then delivers it to the intended recipient.

- **Quarantine message to server-side spam folder**

The Messaging Security Agent moves the message to the server side quarantine folder.

Approved and Blocked Senders Lists

An Approved Senders list is a list of trusted email addresses. The MSA does not filter messages arriving from these addresses for spam except when **Detect Phishing incidents** is enabled. When you have enabled **Detect Phishing incidents**, and the MSA detects a phishing incident in an email, then that email message will not be delivered even when it belongs to an approved sender list. A Blocked Senders list is a list of suspect email addresses. The MSA always categorizes email messages from blocked senders as spam and takes the appropriate action.

There are two Approved Senders lists: one for the Microsoft Exchange Administrator and one for the end-users.

- The Microsoft Exchange Administrator's Approved Senders list and Blocked Senders list (on the **Anti-spam** screen) control how the MSA handles email messages bound for the Microsoft Exchange server.

- The end-user manages the Spam Folder that is created for them during installation. The end-users' lists only affect the messages bound for the server-side mailbox store for each individual end-user.

Note: Approved and Blocked Senders lists on a Microsoft Exchange server override the Approved and Blocked Senders lists on a client. For example, the sender "user@example.com" is on the Administrator's Blocked Senders list, but the end-user has added that address to his Approved Senders list. Messages from that sender arrive at the Microsoft Exchange store and the MSA detects them as spam and takes action against them. If the MSA takes the *Quarantine message to user's spam folder* action, it will attempt to deliver the message to the end user's Spam folder, but the message will be redirected to the end user's inbox instead because the end user has approved that sender.

Note: When you are using Outlook, there is a size limit for the amount and size of addresses on the list. To prevent a system error, the MSA limits the amount of addresses that an end user can include in his or her approved sender list (this limit is calculated according to the length and the number of email addresses).

Wildcard matching

The MSA supports wildcard matching for Approved and Blocked Senders lists. It uses the asterisk (*) as the wildcard character.

The MSA does not support the wildcard match on the user name part. However, if you type a pattern such as "*@trend.com", the MSA still treats it as "@trend.com".

You can only use a wildcard if it is:

- next to only one period and the first or last character of a string
- to the left of an @ sign and the first character in the string

- any missing section at the beginning or end of the string serves the same function as a wildcard

TABLE 9-3. Email Address Matches for Wildcards

PATTERN	MATCHED SAMPLES	UNMATCHED SAMPLES
john@example.com	john@example.com	Any address different from the pattern
@example.com *@example.com	john@example.com mary@example.com	john@ms1.example.com john@example.com.us mary@example.com.us
example.com	john@example.com john@ms1.example.com mary@ms1.rd.example.com mary@example.com	john@example.com.us mary@myexample.com.us joe@example.comon
*.example.com	john@ms1.example.com mary@ms1.rd.example.com joe@ms1.example.com	john@example.com john@myexample.com.us mary@ms1.example.comon
example.com.*	john@example.com.us john@ms1.example.com.us john@ms1.rd.example.com.us mary@example.com.us	john@example.com mary@ms1.example.com john@myexample.com.us
.example.com.	john@ms1.example.com.us john@ms1.rd.example.com.us mary@ms1.example.com.us	john@example.com john@ms1.example.com john@trend.example.us

TABLE 9-3. Email Address Matches for Wildcards (Continued)

PATTERN	MATCHED SAMPLES	UNMATCHED SAMPLES
*. *. *.example.com *****.example.com	The same as "*.example.com"	
example.com example.com example.*.com @*.example.com	Invalid patterns	

To set up a list of Approved Senders:

1. Type an email address in the field provided in the **Approved Senders** group box.
2. Click **Add**. The address is added to the Approved Senders list.
3. Click **Save**. The list identified by file directory is imported into your Messaging Security Agent Approved Senders list.
- Or -
Click **Import**. The Anti-Spam Import File screen appears.
4. Type a directory path that specifies the location of the list that you want to import or click Browse and navigate to the file.
5. Click **Save**. The list that you specified is imported into your Messaging Security Agent Approved Senders list.

To set up a list of Blocked Senders

1. Type an email address in the field provided in the **Blocked Senders** group box.
2. Click **Add**. The address is added to the Blocked Senders list.
3. Click **Save**. The list identified by file directory is imported into your Messaging Security Agent Blocked Senders list.
- Or -
Click **Import**. The Anti-Spam Import File screen appears.

4. Type a directory path that specifies the location of the list that you want to import or click **Browse** and navigate to the file.
5. Click **Save**. The list that you specified is imported into your Messaging Security Agent Blocked Senders list.

Configuring Content Scanning

Navigation Path: Security Settings > {MSA} > Configure > Anti-Spam > Content Scanning

Configuring Content Scanning to scan SMTP traffic for spam is a two-step process. First, select a spam detection level, configure the Approved Senders, and Blocked Senders lists. Next, choose the action for to take when WFBS detects spam.

FIGURE 9-3. Content Scanning screen

To configure Content Scanning:

1. From the **Target** tab on the Content Scanning screen, update the following as required:
 - Enable real-time Anti-Spam (Content Scanning)

- **Spam Detection Level:** See *Spam Detection* on page 9-30.
- **Detect Phishing:** Phishing incidents encourage users to click a link that will redirect their browser to a fraudulent website that imitates an authentic website. See *Phishing* on page 9-31.
- **Approved Senders:** Email messages from these addresses or domain names will never be blocked. Type the addresses or domain names to approve and click Add. If required, you can import a list of addresses or domain names from a text file. To remove addresses or domain names, select the address and click Remove. See *Approved and Blocked Senders Lists* on page 9-33.
- **Blocked Senders:** Email messages from these addresses or domain names will always be blocked. Type the addresses or domain names to block and click **Add**. If required, you can import a list of addresses or domain names from a text file. To remove addresses or domain names, select the address and click **Remove**. See *Approved and Blocked Senders Lists* on page 9-33.

Note: The **Blocked IP Addresses list** takes precedence over **Content Scanning**.

2. Click **Save**.
3. From the **Action** tab on the Content Scanning screen, update the following as required:
 - **Spam**
 - **Quarantine message to server-side spam folder**
 - **Quarantine message to user's spam folder**
 - **Delete entire message**
 - **Tag and deliver:** Appends the tag to the subject of the email message.
 - **Phishing Incident**
 - **Quarantine message to server-side spam folder**
 - **Delete entire message**
 - **Tag and deliver:** Appends the tag to the subject of the email message.
4. Click **Save**.

Content Filtering

Navigation Path: Security Settings > {MSA} > Configure > Content Filtering > Add {or click rule to Edit}

Content Filtering evaluates inbound and outbound email 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 Microsoft Exchange clients. The Messaging Security Agent can send notifications whenever it takes an action against undesirable content.

Note: Do not confuse Content Scanning (anti-spam based on signatures and heuristics) with Content Filtering (email scanning and blocking based on categorized keywords). See [Content Scanning](#) on page 9-30.

The content filter provides a means for the Administrator to evaluate and control the delivery of email 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 harassing language
- Racist language
- Spam embedded in the body of an email message

Note: By default, content filtering is not enabled.

After you have created your rule, the Messaging Security Agent (MSA) begins to filter all incoming and outgoing messages according to your rule. You can create rules that can:

- **Filter messages that match any condition defined:** This type of rule is capable of filtering content from any message during a scan.
- **Filter messages that match all conditions defined:** This type of rule is capable of filtering content from any message during a scan.

- **Monitor the message content of particular email accounts:** This type of rule monitors the message content of particular email accounts. Monitoring rules are similar to a general content filter rules, except that they only filter content from specified email accounts.
- **Create exceptions for particular email accounts:** This type of rule creates an exception for particular email accounts. When you exempt a particular email account, this account will not be filtered for content rule violations.

Scan Actions

During Content Filtering, if an email message matches a rule, any one of the following actions can be configured:

- **Replace with text/file:** Replaces the filtered content with a text file. You cannot replace text from the **From**, **To**, **Cc**, or **Subject** fields.
- **Quarantine entire message:** Moves the entire message to the quarantine directory.
- **Quarantine message part:** Quarantines only the filtered content to the quarantine directory and the recipient receives the message without this content.
- **Delete entire message:** Deletes the entire email message.
- **Archive:** Moves the message to the archive directory and delivers the message to the original recipient.
- **Pass:** Delivers the message as is.

Note: The quarantine action is unavailable during Manual or Scheduled Scans.

To create/edit a rule:

1. From the **Content Filtering** screen, click **Add**.
To edit a rule, click the name of the rule.
2. Select the type of rule and click **Next**.
3. To filter messages that match any condition defined:
 - a. Name the rule.
 - b. Set the scan conditions.
 - c. Add the keywords. Include synonyms and/or case-sensitive criteria.

- d. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.
4. To filter messages that match all conditions defined:
 - a. Name the rule.
 - b. Set the scan conditions.
 - c. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.
5. To monitor the message content of particular email accounts
 - a. Name the rule.
 - b. Set the accounts to monitor.
 - c. Set the scan conditions.
 - d. Add the keywords. Include synonyms and/or case-sensitive criteria.
 - e. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.
6. To create an exception list for email accounts
 - a. Name the rule.
 - b. Set the accounts to exclude.

Note: The Messaging Security Agent does not apply content rules with a lower priority than this rule to email accounts in this list.

7. Click **Finish**.

Adding/Editing Content Filtering Rules

Navigation Path: Security Settings > {MSA} > Configure > Content Filtering > Add/Edit a Rule

After you have created your rule, the Messaging Security Agent (MSA) begins to filter all incoming and outgoing messages according to your rule. You can create rules that can:

- **Filter messages that match any condition defined:** This type of rule is capable of filtering content from any message during a scan.
- **Filter messages that match all conditions defined:** This type of rule is capable of filtering content from any message during a scan.
- **Monitor the message content of particular email accounts:** This type of rule monitors the message content of particular email accounts. Monitoring rules are similar to a general content filter rules, except that they only filter content from specified email accounts.
- **Create exceptions for particular email accounts:** This type of rule creates an exception for particular email accounts. When you exempt a particular email account, this account will not be filtered for content rule violations.

To create/edit a rule:

1. From the **Content Filtering** screen, click **Add**.
To edit a rule, click the name of the rule.
2. Select the type of rule and click **Next**.
3. To filter messages that match any condition defined:
 - a. Name the rule.
 - b. Set the scan conditions.
 - c. Add the keywords. Include synonyms and/or case-sensitive criteria.
 - d. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.
4. To filter messages that match all conditions defined:
 - a. Name the rule.
 - b. Set the scan conditions.
 - c. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.
5. To monitor the message content of particular email accounts
 - a. Name the rule.
 - b. Set the accounts to monitor.
 - c. Set the scan conditions.

- d. Add the keywords. Include synonyms and/or case-sensitive criteria.
 - e. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.
6. To create an exception list for email accounts
 - a. Name the rule.
 - b. Set the accounts to exclude.

Note: The Messaging Security Agent does not apply content rules with a lower priority than this rule to email accounts in this list.

7. Click **Finish**.

Creating Content Filtering Rules

Navigation Path: Security Settings > {MSA} > Configure > Content filtering

You can create rules that filter email messages according to the conditions you specify or according to the email addresses of the sender or recipient. Conditions you can specify in the rule include: which header fields to scan, whether or not to search the body of an email message, and what keywords to search for.

When a content violation occurs, the Messaging Security Agent takes action against the violating email message. The action that the Security Server takes also depends on the actions that you set in your rule. Finally, you can set some email addresses as exempt from content filtering.

To create a new rule, click **Add**. A wizard launches. It provides step-by-step instructions for you to follow to set up the rule. You can set up one of four types of rules and a custom wizard guides you through each one.

To create a content filtering monitoring rule:

1. Select the type of rule:
 - Select Monitor the message content of particular email accounts to monitor email messages sent from and/or to a specified account.

2. Name your rule:
 - a. Type the name of your rule in the Rule name space.
 - b. Select the message part that you want to filter for undesirable content. The Messaging Security Agent can filter email messages by the **From**, **To**, and **Cc** parts of the email message.
 - c. The Messaging Security Agent only supports filtering of these parts of the email message during real-time scan. It does not support filtering of header and subject content during manual and scheduled scans.
 - d. Click **Next**.
3. Set the action
 - a. Select an action for the Messaging Security Agent to take when it detects undesirable content. The Messaging Security Agent can perform the following actions when it detects content that matches the rule conditions:
 - **Replace with text/file:** Replaces the filtered content with a text file. You cannot replace text from the From, To, Cc, or subject fields.
 - **Quarantine entire message:** Moves the message to the quarantine directory.
 - **Quarantine message part:** Quarantines only the filtered content to the quarantine directory and the recipient receives the message without this content.
 - **Delete entire message:** Deletes the entire email message.
 - **Archive:** Delivers archived mail to the intended recipient and keeps a copy of the message in the specified archive directory.
 - b. Select **Notify recipients** to set the Messaging Security Agent to notify the intended recipients of email messages that had content filtered.

Select **Do not notify external recipients** to only send notifications to internal mail recipients. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.
 - c. Select **Notify senders** to set the Messaging Security Agent to notify the senders of email messages that had content filtered.

Select **Do not notify external senders** to only send notifications to internal mail senders. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

- d. Click **Finish**. The wizard closes and returns to the Content Filtering screen.

Creating Content Filtering Rules for All Matching Conditions

Navigation Path: Security Settings > {MSA} > Configure > Content filtering

To create a new rule, click **Add**. A wizard launches. It provides step-by-step instructions for you to follow to set up the rule. You can set up one of four types of rules and a custom wizard guides you through each one.

To create a content filtering rule for all matching conditions:

1. Select a type of rule:
 - Select **Filter message that match all conditions defined** to have the Messaging Security Agent take action only when an email message violates all of the conditions in your rule.
2. Name your rule:
 - a. Type the name of your rule in the **Rule name** field.
 - b. Select the message part that you want to filter for undesirable content. The Messaging Security Agent can filter email messages by Header (**From**, **To**, and **Cc**), **Subject**, **Body**, or **Attachment**.

Note: The Messaging Security Agent only supports filtering of header and subject content during real-time scan.

- c. Click **Next**.
3. Set the action:
 - a. Select an action for the Messaging Security Agent to take when it detects undesirable content. The Messaging Security Agent can perform the following actions when it detects content that matches the rule conditions:

- **Replace with text/file:** Replaces the filtered content with a text file. You cannot replace text from the **From**, **To**, **Cc**, or subject fields.
 - **Quarantine entire message:** Moves the message to the quarantine directory.
 - **Quarantine message part:** Quarantines only the filtered content to the quarantine directory and the recipient receives the message without this content.
 - **Delete entire message:** Deletes the entire email message.
 - **Archive:** delivers archived mail to the intended recipient and keeps a copy of the message in the specified archive directory
- b. Select **Notify recipients** to set the Messaging Security Agent to notify the intended recipients of email messages that had content filtered.
- Select **Do not notify external recipients** to only send notifications to internal mail recipients. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.
- c. Select **Notify senders** to set the Messaging Security Agent to notify the senders of email messages that had content filtered.
- Select **Do not notify only external senders** to only send notifications to internal mail senders. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.
- d. Click **Finish**. The wizard closes and returns to the Content Filtering screen.

Creating Exceptions to Content Filtering Rules

Navigation Path: Security Settings > {MSA} > Configure > Content Filtering > Add

To create a new rule, click **Add**. A wizard launches. It provides step-by-step instructions for you to follow to set up the rule. You can set up one of four types of rules and a custom wizard guides you through each one.

To create a content filtering rule:

1. From the Content Filtering page, click **Add**.
2. Select **Create exemption for particular email accounts** to exempt a particular email account.
3. This option is useful when you want to exempt a person who has special privileges or represents no security risk
4. Click **Next**.
5. Type a rule name.
6. Type the email accounts that you want to exempt from content filtering in the space provided and click Add. The email account is added to your list of exempt email accounts.
7. When you are satisfied with your list of email accounts, click Finish. The wizard closes and returns you to the Content Filtering screen.

Editing Content Filtering Rules

Navigation Path: Security Settings > {MSA} > Configure > Content filtering > {rule}

You can modify a rule by clicking on the rule name from the Content Filtering screen. When you click a rule name, the Edit Rule screen opens displaying information that corresponds to that rule.

You can modify the following target parts of a rule:

- Enable or disable the rule
- Modify the rule name
- Modify the keywords for which the Messaging Security Agent searches
- Modify the target part of the email message that the Messaging Security Agent filters
- Set the action the Messaging Security Agent takes against content that matches the keyword

To enable or disable content filtering rules:

- To enable all the content filtering rules, except individually disabled rules, select Enable Content Filtering from Content Filtering screen. Clearing the check box disables all Content Filtering rules.

- To enable an individual rule:

Click a rule to open the Edit Rule screen

Select **Enable this rule**. Clearing this check box disables the rule.

To enable or disable an individual rule:

- Click an enable icon to disable the rule that matches the icon. The icon will toggle from enable to disable to show the new status.
- Click a disable icon to enable the rule that matches the icon. The icon will toggle from disable to enable to show the new status.

To modify the rule name:

1. Click a rule to open the Edit Rule screen.
2. Type a new name in the Rule name field.
3. Click **Save**.

To modify the target part of the email message that the Messaging Security Agent filters:

1. Click a rule to open the Edit Rule screen.
2. Choose the target parts of the email that you want to modify. Different rules are able to filter different target parts of the email message. Refer to the procedure for creating each type of rule for detailed information about the target parts of the message that it can filter.
3. Modify the keywords for the target part that you want to filter for undesirable content. If necessary, select whether or not to make content filter case-sensitive. Import new keyword files as needed.
4. Click **Save**.

To modify the action that the Messaging Security Agent takes when it detects a Content Rule violation:

1. Click a rule to open the Edit Rule screen.
2. Click the **Action** tab.
3. Select an action for the Messaging Security Agent to take when it detects undesirable content.
4. Set the Messaging Security Agent to notify the original recipients of the filtered email message.

5. Click **Save**.

To modify the keywords for which the Messaging Security Agent searches:

1. Click a rule to open the Edit Rule screen.
2. Select a keyword from the Keyword list.
3. Click **Delete** to remove it from the list.
4. Display the list of synonyms. When you select a keyword, all of the keyword's synonyms display in the **Synonyms to exclude** list. Use the arrow keys to add or delete synonyms for each corresponding keyword.
5. Click **Save**.

Removing Content Filtering Rules

When you delete a rule, the Messaging Security Agent updates the order of the other rules to reflect the change.

Note: Deleting a rule is irreversible, consider disabling a rule instead of deleting.

To delete a rule:

1. Click **Security Settings > {MSA or group}**.
2. Click **Configure > Content filtering**.
3. From the Content Filtering screen, select a rule.
4. Click **Remove**.

Keywords

In WFBS, keywords include the following and are used to filter messages:

- Words (guns, bombs, and so on)
- Numbers (1,2,3, and so on)
- Special characters (&,#,+, and so on)
- Short phrases (blue fish, red phone, big house, and so on)

- Words or phrases connected by logical operators (apples .AND. oranges)
- Words or phrases that use *regular expressions* (.REG. a.*e matches “ace”, “ate”, and “advance”, but not “all”, “any”, or “antivirus”)

Importing Keywords

WFBS can import an existing list of keywords from a text (.txt) file. Imported keywords appear in the keyword list.

Using Operators on Keywords

Operators are commands that combine multiple keywords. Operators can broaden or narrow the results of a criteria. Enclose operators with periods (.). For example,

apples .AND. oranges and apples .NOT. oranges

Note: The operator has a dot immediately preceding and following. There is a space between the final dot and the keyword.

TABLE 9-4. Using Operators

OPERATOR	HOW IT WORKS	EXAMPLE
any keyword	The MSA searches content that matches the word	Type the word and add it to the keyword list
OR	The MSA searches for any of the keywords separated by OR For example, apple OR orange. The MSA searches for either apple or orange. If content contains either, then there is a match.	Type ".OR." between all the words you want to include For example, "apple .OR. orange"

TABLE 9-4. Using Operators (Continued)

OPERATOR	HOW IT WORKS	EXAMPLE
AND	The MSA searches for all of the keywords separated by AND For example, apple AND orange. The MSA searches for both apple and orange. If content does not contain both, then there is no match.	Type ".AND." between all the words you want to include For example, "apple .AND. orange"
NOT	The MSA excludes keywords following NOT from search. For example, .NOT. juice. The MSA searches for content that does not contain juice. If the message has "orange soda", there is a match, but if it contains "orange juice", there is no match.	Type ".NOT." before a word you want to exclude For example, ".NOT. juice"
WILD	The wildcard symbol replaces a missing part of the word. Any words that are spelled using the remaining part of the wildcard are matched. Note: The MSA does not support using "?" in the wildcard command ".WILD.".	Type ".WILD." before the parts of the word you want to include For example, if you want to match all words containing "valu", type ".WILD.valu". The words Valumart, valucash, and valubucks all match.

TABLE 9-4. Using Operators (Continued)

OPERATOR	HOW IT WORKS	EXAMPLE
REG	To specify a <i>regular expression</i>, add a .REG. operator before that pattern (for example, .REG. a.*e). See Regular Expressions on page 9-55.	Type ".REG." before the word pattern you want to detect. For example, ".REG. a.*e" matches: "ace", "ate", and "advance", but not "all", "any", nor "antivirus"

Using Keywords Effectively

The Messaging Security Agent offers simple and powerful features to create highly specific filters. Consider the following, when creating your Content Filtering rules:

- By default, the MSA searches for exact matches of keywords. Use *regular expressions* to set MSA to search for partial matches of keywords. See [Regular Expressions](#) on page 9-55.
- The MSA analyzes multiple keywords on one line, multiple keywords with each word on a separate line, and multiple keywords separated by commas/periods/hyphens/and other punctuation marks differently. See [Table 9-5](#) for more information about using keywords on multiple lines.
- You can also set the MSA to search for synonyms of the actual keywords.

TABLE 9-5. How to Use Keywords

SITUATION	EXAMPLE	MATCH/NON-MATCH
Two words on same line	guns bombs	Matches: "Click here to buy guns bombs and other weapons." Does not match: "Click here to buy guns and bombs."

TABLE 9-5. How to Use Keywords (Continued)

SITUATION	EXAMPLE	MATCH/NON-MATCH
Two words separated by a comma	guns, bombs	Matches: "Click here to buy guns, bombs, and other weapons." Does not match: "Click here to buy used guns, new bombs, and other weapons."

TABLE 9-5. How to Use Keywords (Continued)

SITUATION	EXAMPLE	MATCH/NON-MATCH
Multiple words on multiple lines	guns bombs weapons and ammo	When you choose Any specified keywords Matches: “Guns for sale” Also matches: “Buy guns, bombs, and other weapons” When you choose All specified keywords Matches: “Buy guns bombs weapons and ammo” Does not match: “Buy guns bombs weapons ammunition.” Also does not match: “Buy guns, bombs, weapons, and ammo”
Many keywords on same line	guns bombs weapons ammo	Matches: “Buy guns bombs weapons ammo” Does not match: “Buy ammunition for your guns and weapons and new bombs”

Regular Expressions

Regular expressions are used to perform string matching. See the following tables for some common examples of regular expressions. To specify a *regular expression*, add a “.REG.” operator before that pattern.

There are a number of websites and tutorials available online. One such site is the PerlDoc site, which can be found at:

<http://www.perl.com/doc/manual/html/pod/perlre.html>

WARNING! Regular expressions are a powerful string matching tool. For this reason, Trend Micro recommends that Administrators who choose to use regular expressions be familiar and comfortable with regular expression syntax. Poorly written regular expressions can have a dramatic negative performance impact. Trend Micro recommends is to start with simple regular expressions that do not use complex syntax. When introducing new rules, use the archive action and observe how the MSA manages messages using your rule. When you are confident that the rule has no unexpected consequences, you can change your action.

See the following tables for some common examples of regular expressions. To specify a *regular expression*, add a “.REG.” operator before that pattern.

TABLE 9-6. Counting and Grouping

ELEMENT	WHAT IT MEANS	EXAMPLE
.	The dot or period character represents any character except new line character.	do. matches doe, dog, don, dos, dot, etc.d.r matches deer, door, etc.
*	The asterisk character means zero or more instances of the preceding element.	do* matches d, do, doo, dooo, doooo, etc.
+	The plus sign character means one or more instances of the preceding element.	do+ matches do, doo, dooo, doooo, etc. but not d

TABLE 9-6. Counting and Grouping (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
?	The question mark character means zero or one instances of the preceding element.	<code>do?g</code> matches <code>dg</code> or <code>dog</code> but not <code>doog</code> , <code>dooog</code> , etc.
()	Parenthesis characters group whatever is between them to be considered as a single entity.	<code>d(eer)+</code> matches <code>deer</code> or <code>deereer</code> or <code>deereereer</code> , etc. The + sign is applied to the substring within parentheses, so the regex looks for <code>d</code> followed by one or more of the grouping “ <code>eer</code> .”
[]	Square bracket characters indicate a set or a range of characters.	<code>d[aeiouy]+</code> matches <code>da</code> , <code>de</code> , <code>di</code> , <code>do</code> , <code>du</code> , <code>dy</code> , <code>daa</code> , <code>dae</code> , <code>dai</code> , etc. The + sign is applied to the set within brackets parentheses, so the regex looks for <code>d</code> followed by one or more of any of the characters in the set <code>[aeiouy]</code> . <code>d[A-Z]</code> matches <code>dA</code> , <code>dB</code> , <code>dC</code> , and so on up to <code>dZ</code> . The set in square brackets represents the range of all upper-case letters between <code>A</code> and <code>Z</code> .
[^]	Carat characters within square brackets logically negate the set or range specified, meaning the regex will match any character that is not in the set or range.	<code>d[^aeiouy]</code> matches <code>db</code> , <code>dc</code> or <code>dd</code> , <code>d9</code> , <code>d#</code> -- <code>d</code> followed by any single character except a vowel.

TABLE 9-6. Counting and Grouping (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
{ }	Curly brace characters set a specific number of occurrences of the preceding element. A single value inside the braces means that only that many occurrences will match. A pair of numbers separated by a comma represents a set of valid counts of the preceding character. A single digit followed by a comma means there is no upper bound.	da{3} matches daaa--d followed by 3 and only 3 occurrences of "a". da{2,4} matches daa, daaa, daaaa, and daaaa (but not daaaaa)--d followed by 2, 3, or 4 occurrences of "a". da{4,} matches daaaa, daaaaa, daaaaaa, etc.--d followed by 4 or more occurrences of "a".

TABLE 9-7. Character Classes (shorthand)

ELEMENT	WHAT IT MEANS	EXAMPLE
\d	Any digit character; functionally equivalent to [0-9] or [[:digit:]]	\d matches 1, 12, 123, etc., but not 1b7--one or more of any digit characters.
\D	Any non-digit character; functionally equivalent to [^0-9] or [^[:digit:]]	\D matches a, ab, ab&, but not 1--one or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.
\w	Any "word" character--that is, any alphanumeric character; functionally equivalent to [_A-Za-z0-9] or [[:alnum:]]	\w matches a, ab, a1, but not !&--one or more upper- or lower-case letters or digits, but not punctuation or other special characters.
\W	Any non-alphanumeric character; functionally equivalent to [^_A-Za-z0-9] or [^[:alnum:]]	\W matches *, &, but not ace or a1--one or more of any character but upper- or lower-case letters and digits.

TABLE 9-7. Character Classes (shorthand) (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
\s	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to <code>[[:space]]</code>	<code>vegetable\s</code> matches “vegetable” followed by any white space character. So the phrase “I like a vegetable in my soup” would trigger the regex, but “I like vegetables in my soup” would not.
\S	Any non-white space character; anything other than a space, new line, tab, non-breaking space, etc.; functionally equivalent to <code>[^[:space]]</code>	<code>vegetable\S</code> matches “vegetable” followed by any non-white space character. So the phrase “I like vegetables in my soup” would trigger the regex, but “I like a vegetable in my soup” would not.

TABLE 9-8. Character Classes

ELEMENT	WHAT IT MEANS	EXAMPLE
<code>[[:alpha:]]</code>	Any alphabetic characters	<code>.REG. [[:alpha:]]</code> matches <code>abc</code> , <code>def</code> , <code>xxx</code> , but not <code>123</code> or <code>@#\$</code> .
<code>[[:digit:]]</code>	Any digit character; functionally equivalent to <code>\d</code>	<code>.REG. [[:digit:]]</code> matches <code>1</code> , <code>12</code> , <code>123</code> , etc.
<code>[[:alnum:]]</code>	Any “word” character--that is, any alphanumeric character; functionally equivalent to <code>\w</code>	<code>.REG. [[:alnum:]]</code> matches <code>abc</code> , <code>123</code> , but not <code>~!@</code> .
<code>[[:space:]]</code>	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to <code>\s</code>	<code>.REG. (vegetable)[[:space:]]</code> matches “vegetable” followed by any white space character. So the phrase “I like a vegetable in my soup” would trigger the regex, but “I like vegetables in my soup” would not.

TABLE 9-8. Character Classes (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
<code>[:graph:]</code>	Any characters except space, control characters or the like	.REG. <code>[:graph:]</code> matches 123, abc, xxx, ><, but not space or control characters.
<code>[:print:]</code>	Any characters (similar with <code>[:graph:]</code>) but includes the space character	.REG. <code>[:print:]</code> matches 123, abc, xxx, ><, and space characters.
<code>[:cntrl:]</code>	Any control characters (e.g. CTRL + C, CTRL + X)	.REG. <code>[:cntrl:]</code> matches 0x03, 0x08, but not abc, 123, !@#.
<code>[:blank:]</code>	Space and tab characters	.REG. <code>[:blank:]</code> matches space and tab characters, but not 123, abc, !@#
<code>[:punct:]</code>	Punctuation characters	.REG. <code>[:punct:]</code> matches ; : ? ! ~ @ # \$ % & * ' " , etc., but not 123, abc
<code>[:lower:]</code>	Any lowercase alphabetic characters (Note: 'Enable case sensitive matching' must be enabled or else it will function as <code>[:alnum:]</code>)	.REG. <code>[:lower:]</code> matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, !@#.
<code>[:upper:]</code>	Any uppercase alphabetic characters (Note: 'Enable case sensitive matching' must be enabled or else it will function as <code>[:alnum:]</code>)	.REG. <code>[:upper:]</code> matches ABC, DEF, STRESS, DO, etc., but not abc, Def, Stress, Do, 123, !@#.
<code>[:xdigit:]</code>	Digits allowed in a hexadecimal number (0-9a-fA-F)	.REG. <code>[:xdigit:]</code> matches 0a, 7E, 0f, etc.

TABLE 9-9. Pattern Anchors

ELEMENT	WHAT IT MEANS	EXAMPLE
^	Indicates the beginning of a string.	^(notwithstanding) matches any block of text that began with “notwithstanding” So the phrase “notwithstanding the fact that I like vegetables in my soup” would trigger the regex, but “The fact that I like vegetables in my soup notwithstanding” would not.
\$	Indicates the end of a string	(notwithstanding)\$ matches any block of text that ended with “notwithstanding” So the phrase “notwithstanding the fact that I like vegetables in my soup” would not trigger the regex, but “The fact that I like vegetables in my soup notwithstanding” would.

TABLE 9-10. Escape Sequences and Literal Strings

ELEMENT	WHAT IT MEANS	EXAMPLE
\	In order to match some characters that have special meaning in regular expression (for example, “+”).	(1) .REG. C\\C\\+\\+ matches ‘C\\C++’. (2) .REG. * matches *. (3) .REG. \\? matches ?.
\\t	Indicates a tab character.	(stress)\\t matches any block of text that contained the substring “stress” immediately followed by a tab (ASCII 0x09) character.

TABLE 9-10. Escape Sequences and Literal Strings (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
\n	Indicates a new line character. NOTE: Different platforms represent a new line character. On Windows, a new line is a pair of characters, a carriage return followed by a line feed. On Unix and Linux, a new line is just a line feed, and on Macintosh a new line is just a carriage return.	(stress)\n\n matches any block of text that contained the substring “stress” followed immediately by two new line (ASCII 0x0A) characters.
\r	Indicates a carriage return character.	(stress)\r matches any block of text that contained the substring “stress” followed immediately by one carriage return (ASCII 0x0D) character.
\b	Indicates a backspace character. OR Denotes boundaries	(stress)\b matches any block of text that contained the substring “stress” followed immediately by one backspace (ASCII 0x08) character. A word boundary (\b) is defined as a spot between two characters that has a \w on one side of it and a \W on the other side of it (in either order), counting the imaginary characters off the beginning and end of the string as matching a \W. (Within character classes \b represents backspace rather than a word boundary.) For example, the following regular expression can match the social security number: .REG. \b\d{3}-\d{2}-\d{4}\b

TABLE 9-10. Escape Sequences and Literal Strings (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
\xhh	Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).	\x7E(\w){6} matches any block of text containing a “word” of exactly six alphanumeric characters preceded with a ~ (tilde) character. So, the words '~ab12cd', '~Pa3499' would be matched, but '~oops' would not.

Using Complex Expression Syntax

A keyword expression is composed of tokens, which is the smallest unit used to match the expression to the content. A token can be an operator, a logical symbol, or the operand, i.e., the argument or the value on which the operator acts.

Operators include .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., “. (.” and “.).” The operand and the operator must be separated by a space. An operand may also contain several tokens. See [Keywords](#) on page 9-49.

Regular Expression Example

The following example describes how the Social Security content filter, one of the default filters, works:

```
[Format] .REG. \b\d{3}-\d{2}-\d{4}\b
```

The above expression uses **\b**, a backspace character, followed by **\d**, any digit, then by **{x}**, indicating the number of digits, and finally, **-**, indicating a hyphen. This expressions matches with the social security number. The following table describes the strings that match the example regular expression:

TABLE 9-11. Numbers matching the Social Security Regular Expression

.REG. \b\d{3}-\d{2}-\d{4}\b	
333-22-4444	Match
333224444	Not a match

TABLE 9-11. Numbers matching the Social Security Regular Expression (Continued)

.REG. \b\d{3}-\d{2}-\d{4}\b	
333 22 4444	Not a match
3333-22-4444	Not a match
333-22-44444	Not a match

If you modify the expression as follows,

[Format] .REG. \b\d{3}\x20\d{2}\x20\d{4}\b

the new expression matches the following sequence:

333 22 4444

Viewing Content Filtering Rules

Navigation Path: Security Settings > {MSA} > Configure > Content Filtering

The Messaging Security Agent (MSA) displays all the content filtering rules on the Content Filtering screen.

Content Filtering 

☐ Enable real-time content filtering

Rows per page: 10

   1 - 7 of 7 Page 1 of 1

☐ Rule	Action	Priority	Enabled
☐ PROFANITY	Quarantine entire message	1	
☐ RACIAL DISCRIMINATION	Quarantine entire message	2	
☐ SEXUAL DISCRIMINATION	Quarantine entire message	3	
☐ HOAXES	Quarantine entire message	4	
☐ CHAINMAIL	Quarantine entire message	5	
☐ CREDIT CARD NUMBER	Quarantine entire message	6	
☐ SOCIAL SECURITY NUMBER	Quarantine entire message	7	

   1 - 7 of 7 Page 1 of 1

FIGURE 9-4. Content Filtering screen

This screen shows summary information about the rules including:

- **Rule**
- **Action:** The MSA takes this action when it detects undesirable content.
- **Priority:** The MSA applies each filter in succession according to the order shown on this page.
- **Enabled:**  indicates an enabled rule and  indicates a disabled rule.

From here, Administrators can:

- **Enable/disable Content Filtering rules:** Select **Enable real-time content filtering** and click **Save**. This enables or disables all the rules. To enable or disable an individual rule, click  or  to toggle the status of the rule.
- **Add/edit rules:** See *Adding/Editing Content Filtering Rules* on page 9-41.
- **Reorder rules:** See *Reordering Rules* on page 9-65.
- **Remove rules:** Select the rules to delete and click **Remove**.
- **Restore default rules:** This removes all the current rules and restores the default rules. Click **Restore Defaults**.

Reordering Rules

The Messaging Security Agent applies the content filtering rules to email messages according to the order shown in the Content Filtering screen. Configure the order in which the rules are applied. The MSA filters all email messages according to each rule until a content violation triggers an action that prevents further scanning (such as *delete* or *quarantine*). Change the order of these rules to optimize content filtering.

Navigation Path: Security Settings > {MSA} > Configure > Content Filtering >

To change the order of the content filtering rules:

1. From the **Content Filtering** screen, select a check box that corresponds to the rule for which you want to change the order.
2. Click **Reorder**. A box appears around the order number for the rule.
3. Type a new order number in the box. The rule order number will change to the number that you type and all the other rule order numbers will change accordingly. For example, if you select rule number 5 and change it to rule number 3, then rule numbers 1 and 2 will remain the same, and rule numbers 3 and higher will increase by one number.

Data Loss Prevention

Navigation Path: Security Settings > {MSA} > Configure > Data Loss Prevention

You can use Data Loss Prevention to protect against losing data through outgoing email. This feature can protect such data as social security numbers, telephone numbers, bank account numbers, and other confidential business information that matches a set pattern.

The following Exchange versions are supported in this version:

TABLE 9-12. Supported Exchange version

SUPPORTED	NOT SUPPORTED
	Exchange 2003 x86/x64
Exchange 2007 x64	Exchange 2007 x86
Exchange 2010 x64	Exchange 2010 x86

Preparatory Work

Before monitoring sensitive data for potential loss, determine the following:

- Which data needs protection from unauthorized users
- Where the data resides
- Where and how the data is transmitted
- Which users are authorized to access or transmit this information

This important audit typically requires input from multiple departments and personnel familiar with the sensitive information in your organization. The procedures below assume that you have identified the sensitive information and have established security policies regarding handling of confidential business information.

The Worry-Free Data Loss Prevention feature comprises three basic parts:

- **The rules** (patterns to search for): For details, see [Data Loss Prevention Rules](#) on page 9-66.
- **Domains to exclude** from filtering: For details, see [Excluding Specific Domain Accounts](#) on page 9-82.
- **Approved Senders** (email accounts to exclude from filtering): For details, see [Approved Senders](#) on page 9-83.

Data Loss Prevention Rules

Enable the real-time Data Loss Prevention feature at the top of the Data Loss Prevention screen.

Action Bar

From the action bar at the top of the Rules section, you can take five major actions:

- **Add** a rule, as described in [Creating Rules](#) on page 9-69
- **Remove** a rule, as described in [To remove one or more rules:](#) on page 9-78
- **Reorder** (reprioritize) the rules list, as described in [Reordering Rules](#) on page 9-65
- **Import** a set of rules from a text file, as described in [Importing and Exporting Rules](#) on page 9-79
- **Export** a set of rules to a text file, as described in [Importing and Exporting Rules](#) on page 9-79

Kinds of Rules

On the Data Loss Prevention screen upper or lower action bar, click **Add** to add a rule by using either a single keyword or a regular expression, but not both. The method of adding a rule varies greatly depending on which of the three available search criteria you choose:

- **Keyword**, as described in [Adding a Rule Using a Keyword](#) on page 9-69
- **Regular expression (auto-generated)**, as described in [Adding a Rule Using an Auto-Generated Regular Expression](#) on page 9-72
- **Regular expression (user-defined)**, as described in [Adding a Rule Using Your Own Regular Expression](#) on page 9-76

Tip: Move your mouse pointer over the rule name to view the rule. Rules that use a regular expression are flagged with a magnifying glass () icon.

Default Rules

Data Loss Prevention comes with a few default rules, as shown in *Table 9-13. Default Data Loss Prevention rules*.

TABLE 9-13. Default Data Loss Prevention rules

RULE NAME	EXAMPLE	REGULAR EXPRESSION
Visa Card account number	4111-1111-1111-1111	.REG. \b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
MasterCard account number	5111-1111-1111-1111	.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?0?\d{4}\b
American Express account number	3111-111111-1111	.REG. \b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Diners Club/Carte Blanche account number	3111-111111-1111	.REG. [^\d-]((36\d{2} 38\d{2} 30[0-5]\d)\-?\d{6}\-?\d{4})[^\d-]
IBAN	BE68 5390 0754 7034, FR14 2004 1010 0505 0001 3M02 606, DK50 0040 0440 1162 43	.REG. [^\w]((([A-Z]{2})\d{2}[- \s]?)([A-Za-z0-9]{11,27}) ([A-Za-z0-9]{4}[- \s]){3,6}[A-Za-z0-9]{0,3} ([A-Za-z0-9]{4}[- \s]){2}[A-Za-z0-9]{3,4}))[^\w]
Swift BIC	BANK US 99	.REG. [^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-]
ISO date	2004/01/23, 04/01/23, 2004-01-23, 04-01-23	.REG. [^\d\/-]([1-2]\d{3}[-\v][0-1]?\d[-\v][0-3]?\d \d{2}[-\v][0-1]?\d[-\v][0-3]?\d)[^\d\/-]

Note: A zip file containing more DLP rules can be downloaded by clicking the link below the table at **Security Settings > {MSA} > Configure > Data Loss Prevention**.

Creating Rules

Adding a Rule Using a Keyword

You can base a rule on a single keyword. The keyword must be from 1 to 64 alphanumeric characters long.

The Add Rule screen has two major sections:

- Select target
- Add details

To add a keyword rule:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention > Add** to open the Add Rule screen.
2. In the **Select target** section select one or more of the following email fields for the rule to evaluate:
 - **Header (From, To, Cc)**
 - **Subject**
 - **Body**
 - **Attachment**
3. In the **Add details** section select **Keyword**, type the keyword in the field shown, and then click **Next**. A screen appears showing sections for selecting rule action and notification.
4. On the new screen, in the “Select an action” section, choose one of the following actions:

Replace with text/file: Replaces the filtered content with text or with a file. You can replace text only in the body or attachment fields (and not From, To, Cc, or Subject).

Quarantine entire message: Moves the entire message to the quarantine directory set in Step 4 on page 9-70.

Quarantine message part: Quarantines only the filtered content to the quarantine directory, and the recipient receives the message without this content.

Delete entire message.

Archive: Moves the message to the archive directory set in the “Advanced Options” section of this screen and delivers the message to the original recipient.

5. In the “Notification” section, select whether to notify recipients, senders, or both when Data Loss Prevention takes action against a specific email message.

Note: For various reasons, you may want to avoid notifying external mail recipients that a message containing sensitive information was blocked. To turn off notification of external mail recipients, click the plus (+) icon next to **Notify recipients** or **Notify senders** as applicable and then select **Do not notify external recipients** (or senders).

6. Optionally, modify archive settings and replacement settings in the “Advanced Options” section, as explained in *To configure archive and quarantine locations and replacement text*: on page 9-70.
7. Click **Finish** to save your new rule.

To configure archive and quarantine locations and replacement text:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention > Add** to open the Add Rule screen.
2. Fill in the required fields for adding a new rule, as explained in *To add a keyword rule*: on page 9-69.
3. In the Advanced Options section of the Add Rule screen, click the plus (+) icon to expand the **Archive Setting** subsection.
4. In the **Quarantine directory** field, type the path to the folder for Data Loss Prevention to place quarantined email or accept the default value:
C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine
5. Repeat the previous step for the **Archive directory** field.
6. Click the plus (+) icon to expand the **Replacement Settings** subsection.
7. In the **Replacement file name** field, type the name of the file that Data Loss Prevention will replace an email message with when a rule using the “Replace with text/file” action is triggered, or accept the default value:
A_POLICY_VIOLATED_MAIL_WAS_DETECTED_AND_REMOVED.TXT

8. In the **Replacement text** field, type or paste the content of the replacement text for Data Loss Prevention to use when an email message triggers a rule whose action is “Replace with text/file” or accept the default text:
A policy violated content was detected and removed from the original mail header, subject, body or attachment [Attachment Name]. You can safely save or delete this replacement attachment.
9. Click **Finish** to save your new rule.

Things to Consider When Using Regular Expressions with Data Loss Prevention

When deciding how to configure rules for Data Loss Prevention, consider that the regular expression generator can create only simple expressions according to the following rules and limitations:

- ◆ Only alphanumeric characters can be variables.
- ◆ All other characters, such as [-], [/], and so on can only be constants.
- ◆ Variable ranges can only be from A-Z and 0-9; you cannot limit ranges to, say, A-D.
- ◆ Regular expressions generated by this tool are case-insensitive.
- ◆ Regular expressions generated by this tool can only make positive matches, not negative matches (“if does not match”).
- ◆ Expressions based on your sample can only match the exact same number of characters and spaces as your sample; the tool cannot generate patterns that match “one or more” of a given character or string.

Note: The regular expression generator can create only simple expressions. If you need more complex expressions, you can create them manually, as described in [Adding a Rule Using Your Own Regular Expression](#) starting on page 9-76. For more guidance on manually building your own expressions, see [Regular Expressions](#) on page 9-55.

Adding a Rule Using an Auto-Generated Regular Expression

You can use the Data Loss Prevention screen to generate a simple regular expression to use as the filtering criteria for a rule.

Tip: If you need to use a complex regular expression, add it manually by selecting **Regular expression (user-defined)** at the bottom of the “Add details” section of the Data Loss Prevention > Add Rule screen, as explained in [Adding a Rule Using Your Own Regular Expression](#) on page 9-76.

To add a rule using an auto-generated regular expression:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention > Add** to open the Add Rule screen.
2. In the **Select target** section select one or more of the following email fields for the rule to evaluate:
 - **Header (From, To, Cc)**
 - **Subject**
 - **Body**
 - **Attachment**

3. In the **Add details** section, select **Regular expression (auto-generate)**. The screen expands to include several more fields and a tool for generating a regular expression based on sample text, as shown in [Figure 9-5](#).

Add keyword(s)

Enter a specific keyword, Regular Expression, or use an example to generate Regular Expression.

☐ Keyword

☒ **Regular expression (auto-generated)** ⓘ

Rule Name:

Example: (40 characters limit)

☐ Constants ☐ Variables

Regular Expression:

☐ Provide another example to verify the rule (Optional)

☐ Regular expression (user-defined)

FIGURE 9-5. Data Loss Prevention Add Rule screen, Add keyword(s) section, showing expanded area for auto-generation of regular expression

4. In the provided field type a Rule Name. This field is required.
5. In the Example field, type or paste an example of the kind of string (up to 40 characters long) that the regular expression is intended to match. The

alphanumeric characters appear in all caps in the shaded area with rows of boxes beneath the Example field, as shown in [Figure 9-6](#).

The screenshot shows a web interface for creating a regular expression. At the top, there's a section titled "Regular expression (auto-generated)" with an information icon. Below this, there are two input fields: "Rule Name:" containing "Example 2000" and "Example:" containing "01-EXample 2000" with a "(40 characters limit)" note. A shaded area contains a row of character boxes: "0", "1", "-", "E", "X", "A", "M", "P", "L", "E", a space, "2", "0", "0", "0". A mouse cursor is clicking on the last "0" box, which has a "0-9" tooltip. Below the boxes are two checkboxes: "Constants" (unchecked) and "Variables" (unchecked). A text area labeled "Regular Expression:" contains the text ".REG. \b01\-\EX[A-Z]{5}\s20[0-9]{2}\b". At the bottom, there is an unchecked checkbox labeled "Provide another example to verify the rule (Optional)".

FIGURE 9-6. Regular expression (auto-generated) example

6. If there are any constants in the expression, select them by clicking the boxes in which the characters are displayed. As you click each box, its border turns red to indicate that it is a constant and the auto-generation tool modifies the regular expression shown below the shaded area, as shown in [Figure 9-7](#).

This screenshot shows the same interface as Figure 9-6, but with modifications. The "Rule Name:" field still contains "Example 2000" and the "Example:" field contains "01-EXample 2000". In the shaded area, the boxes for "E", "X", "2", and "0" (the first one) now have red borders. Blue arrows point from these boxes to the updated regular expression in the text area below. The regular expression is now ".REG. \b[0-9]{2}\-\EX[A-Z]{5}\s20[0-9]{2}\b". The "Constants" checkbox is still unchecked, and the "Variables" checkbox is also unchecked. The "Provide another example to verify the rule (Optional)" checkbox remains unchecked.

FIGURE 9-7. Regular expression (auto-generated) constants

Note: Non-alphanumeric characters (such as spaces, semicolons, and other punctuation marks) are automatically considered constants and cannot be toggled into variables.

7. To verify that the generated regular expression matches the intended pattern, select **Provide another example to verify the rule (Optional)**. A test field appears below this option, as shown in [Figure 9-8](#).

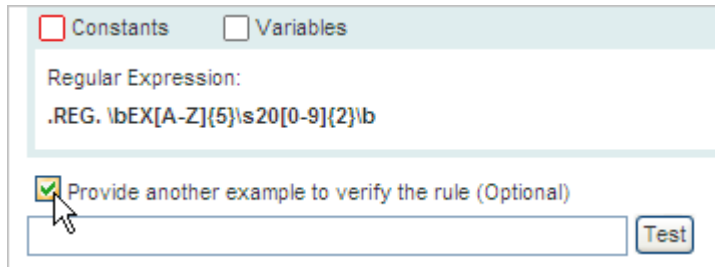


FIGURE 9-8. Regular expression (auto-generated) test field

8. Type another example of the pattern that you just entered. For example, if this expression is to match a series of account numbers of the pattern “01-EX????? 20??”, then type another example that matches, such as “01-Extreme 2010” and then click **Test**. The tool validates the new sample against the existing regular expression and places a green check mark (✓) icon next to the field if the new sample matches. If the regular expression does not match the new sample, a red X icon (✗) appears next to the field.

WARNING! Regular expressions created using this tool are case-insensitive. These expressions can match only patterns with the exact same number of characters as your sample; they cannot evaluate a pattern of “one or more” of a given character.

9. Click **Next**. The Data Loss Prevention > Add Rule screen with “Select an action” and “Notification” sections appears.
10. Finalize the rule by configuring the action, notification, and advanced options sections as explained in steps 4 through 7 on page 9-69.

Adding a Rule Using Your Own Regular Expression

You can use your own regular expressions with Data Loss Prevention rules. You are not limited to auto-generated expressions.

WARNING! Regular expressions are a powerful string-matching tool. Ensure that you are comfortable with regular expression syntax before using these expressions. Poorly written regular expressions can dramatically impact performance. Trend Micro recommends starting with simple regular expressions. When creating new rules, use the “archive” action and observe how Data Loss Prevention manages messages using the rule. When you are confident that the rule has no unexpected consequences, you can change the action.

To add a rule using your own regular expression:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention > Add** to open the Add Rule screen.
2. In the **Select target** section select one or more of the following email fields for the rule to evaluate:
 - **Header (From, To, Cc)**
 - **Subject**
 - **Body**
 - **Attachment**
3. In the **Add details** section, select **Regular expression (user-defined)**. A “Rule Name” and “Regular Expression” field display.
4. In the provided field type a **Rule Name**. This field is required.
5. In the **Regular Expression** field type a regular expression, beginning with a “.REG.” prefix, up to 255 characters long including the prefix.

WARNING! Be very careful when pasting into this field. If any extraneous characters, such as an OS-specific line feed or an HTML tag, is included in the content of your clipboard, the expression pasted will be inaccurate. For this reason, Trend Micro recommends typing the expression by hand.

6. To verify that the regular expression matches the intended pattern, select **Provide another example to verify the rule (Optional)**. A test field appears below this option.
7. Type another example of the pattern that you just entered (40 characters or less). For example, if this expression is to match a series of account numbers of the pattern “ACC-????? 20??” type another example that matches, such as “Acc-65432 2012” and then click **Test**. The tool validates the new sample against the existing regular expression and places a green check mark (✓) icon next to the field if the new sample matches. If the regular expression does not match the new sample, a red X icon (✗) appears next to the field.
8. Click **Next**. The Data Loss Prevention > Add Rule screen with “Select an action” and “Notification” sections appears.
9. Finalize the rule by configuring the action, notification, and advanced options sections as explained in steps 4 through 7 on page 9-69.

Editing a Rule

You can edit an existing rule on the Edit Rule screen. Once you open the Edit Rule screen, the options available to you are exactly the same as those on the Add Rule screen. (See [Creating Rules](#) on page 9-69 for detailed guidance on adding rules.)

To edit a rule:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to display the rules list.
2. If the target rule is not visible on the first page of the rules list, use the page-navigation icons at the top or bottom of the table to turn to the page on which the rule appears.
3. Click the hyperlinked name of the rule in the Rule column. The Edit Rule screen opens.
4. On the Target tab, “Select target” section, modify the email fields to filter by selecting or clearing the fields shown.

5. In the “Add keyword(s)” section, modify the rule in one of the following ways:
 - Change an existing keyword.
 - Select **Regular expression (auto-generated)** and create or modify an expression using the regular expression generator, as described in *To add a rule using an auto-generated regular expression:* on page 9-72.
 - Select **Regular expression (user-defined)** and create or modify a regular expression manually, as described in *To add a rule using your own regular expression:* on page 9-76.
6. On the Action tab, modify any of the settings in the “Select an action,” “Notification,” or “Advanced Options” sections as described in steps 4 through 6 in *To add a keyword rule:* on page 9-69 and in *To configure archive and quarantine locations and replacement text:* on page 9-70.
7. Click **Save**.

Removing, Reprioritizing, Importing, and Exporting Rules

In addition to Add, there are four other action buttons in the Data Loss Prevention screen action bar:

- **Remove:** See *To remove one or more rules:* on page 9-78.
- **Reorder:** See *Reordering Rules* on page 9-65.
- **Import/Export:** See *Importing and Exporting Rules* on page 9-79.

To remove one or more rules:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to display the rules list.
2. Select the rule or rules to remove.
3. In the upper or lower action bar, click **Remove**. Data Loss Prevention immediately (and permanently) removes the selected rules.

WARNING! Before removing a rule, confirm that you no longer need it. There is no “undelete” function. Unless you are completely sure that the rule will never again be needed, it’s a good idea to export the rule to a local file before removing it.

Importing and Exporting Rules

Using the Import and Export action buttons in the action bar at the top of the table on the Data loss Prevention screen, you can import one or more rules from (or export them to) a plain-text file, as shown in [Figure 9-9](#). If you prefer, you can then edit rules directly by using this file.

```
[SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599]
RuleName=Bubbly
UserExample=
Value=Bubbly

[SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6]
RuleName=Master Card No.
UserExample=Value=.REG. \b5[1-5]\d{2}\-\?\x20?\d{4}\-\?\x20?\d{4}\-\?\x20?\d{4}\b
```

FIGURE 9-9. Sample content of a plain-text file created by exporting two rules

To export a rule to a plain-text file:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to display the rules list.
2. Select one or more rules in the list and then click **Export** in the upper or lower action bar of the table. Data Loss Prevention exports the rule in a plain-text file in the format shown in [Figure 9-9](#) on page 9-79.

Tip: You can select rules that appear on one screen only. To select rules that currently appear on different screens, increase the “Rows per page” value at the top of the Rule list table to display enough rows to encompass all of the rules to export.

To import one or more rules from a plain-text file:

1. Create a plain-text file in the format shown in [Figure 9-9](#) on page 9-79 and save it locally.
2. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to display the rules list.

3. In the upper or lower action bar, click **Import**. A Data Loss Prevention Import File window appears, as shown in *Figure 9-10*.

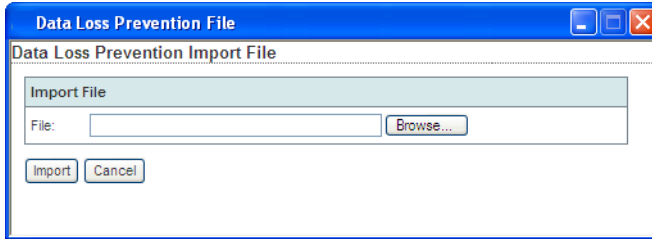


FIGURE 9-10. Import File window

4. Click **Browse** to locate the file to import, and then click **Import**. Data Loss Prevention imports the rules in the file and appends them to the end of the current rules list.

Tip: If you already have more than 10 rules, the imported rules will not be visible on the first page. Use the page-navigation icons at the top or bottom of the rules list to display the last page of the list. The newly imported rules should be there.

Enabling or Disabling a Rule

A newly created rule is by default disabled. There are two ways to enable or disable a rule:

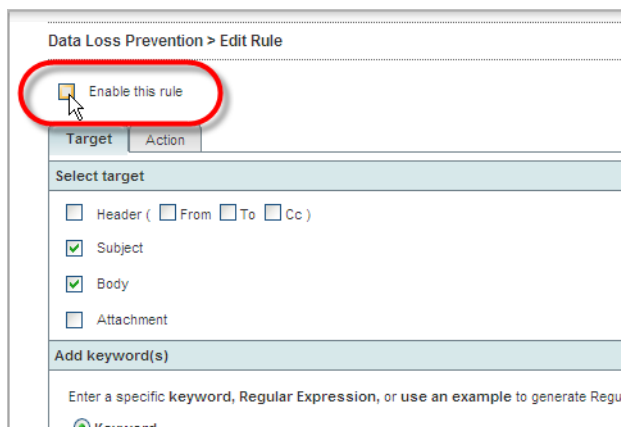
- From the rules list itself
- From within the Edit Rule screen

To enable or disable a rule from the rules list:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to display the rules list.
2. If the target rule is not visible on the first page of the rules list, use the page-navigation icons at the bottom or top of the table to turn to the page on which the rule appears.
3. Select the rule and click the disabled (🛑) or enabled (✅) icon, respectively. The icon toggles to the opposite state, enabling or disabling the selected rule.

To enable or disable a rule from the Edit Rule screen:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to display the rules list.
2. If the target rule is not visible on the first page of the rules list, use the page-navigation icons at the bottom or top of the table to turn to the page on which the rule appears.
3. In the Rule column click the hyperlinked name of the rule. The Edit Rule screen opens.
4. Select or clear the **Enable this rule** check box at the top of the screen, as shown in [Figure 9-11](#).

**FIGURE 9-11.** The “Enable this rule” box on the Edit Rule screen

5. Click **Save**.

Note: Simply selecting or clearing the **Enable this rule** check box does not enable or disable the rule. You must click **Save** to modify the status of the rule.

6. Navigate to the page on which the rule appears and verify that the icon in the “Enabled” column is set to the appearance that you expect (green check mark (✔) icon for enabled, red bar (⊘) icon for disabled).

Pre-approved Domains and Approved Senders

Within the walls of a company, the exchange of confidential business information is a necessary daily occurrence. Also, the processing load on Worry-Free servers would be extreme if Data Loss Prevention had to filter all internal messages. For these reasons, you need to set up one or more default domains, representing your internal company mail traffic, so that Data Loss Prevention does not filter messages sent from one email account to another within your company domain.

Your organization may also have certain email accounts whose outbound messages you do not wish to filter. You can configure Data Loss Prevention to ignore such email accounts.

Excluding Specific Domain Accounts

This list allows all internal email messages (within your company domain) to bypass Data Loss Prevention rules. At least one such domain is required. Add to the list if you use more than one domain.

For example: `*@example.com`

To add a domain for exclusion from Data Loss Prevention filtering:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to open the Data Loss Prevention screen.
2. Click the plus (+) icon to expand the **Specific Domain Account(s) excluded from Data Loss Prevention** section.
3. Place your cursor in the **Add** field and type the domain, using the following pattern:
`*@example.com`

4. Click **Add**. The domain appears in the list shown below the Add field.
5. Click **Save** to complete the process.

WARNING! Data Loss Prevention does not add your domain until you click “Save.” If you click “Add” but not “Save,” your domain will not be added.

Approved Senders

Mail from approved senders travels outside of your network with no filtering by Data Loss Prevention. Add individual email accounts in the **Approved Senders** section of the Data Loss Prevention screen. Data Loss Prevention will ignore the content of any mail sent from email accounts on the approved list.

You may wish to add a long list of email accounts. You can add email accounts individually or import them from a list, as described in [Adding a List of Email Accounts to the Approved Senders List by Importing](#) on page 9-84.

To add an approved sender:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to open the Data Loss Prevention screen.
2. Click the plus (+) icon to expand the **Approved Senders** section.
3. Place your cursor in the **Add** field and type the full email address, using the following pattern: `example@example.com`
4. Click **Add**. The address appears in the list shown below the Add field.
5. Click **Save** to complete the process.

WARNING! Data Loss Prevention does not add the address until you click Save. If you click “Add” but not “Save,” the address will not be added.

Adding a List of Email Accounts to the Approved Senders List by Importing

You can import a list of email addresses from a plain-text file formatted with one email account per line, such as:

```
admin@example.com
ceo@example.com
president@example.com
cfo@example.com
comptroller@example.com
it-admin@example.com
wfbs-admin@example.com
```

FIGURE 9-12. Plain-text file format for importing list of email accounts

To import a list of email addresses from a plain-text file:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to open the Data Loss Prevention screen.
2. Click the plus (+) icon to expand the **Approved Senders** section.
3. Click **Import** (third from the top). The Approved Senders Import File window appears, as shown in [Figure 9-13](#).

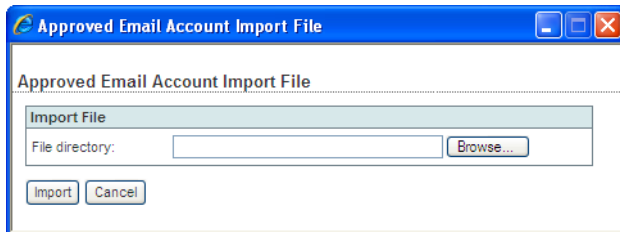


FIGURE 9-13. Approved Senders Import File window

4. Click **Browse** to locate the plain-text file to import, and then click **Import**. Data Loss Prevention imports the rules in the file and appends them to the end of the current list.

Exporting a List of Approved Senders to a Text File

You can also export the list of email accounts in the Approved Senders list.

To export the email accounts in the Approved Senders list to a local text file:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to open the Data Loss Prevention screen.
2. Click the plus (+) icon to expand the **Approved Senders** section.
3. Click **Export**. Data Loss Prevention exports the list to a plain-text file in the format shown in [Figure 9-12](#) on page 9-84.

Note: When exporting email addresses, you can export only the whole list. You cannot select individual accounts to export.

Reordering Data Loss Prevention Rules

The Messaging Security Agent (MSA) applies the Data Loss Prevention rules to email messages according to the order shown on the Rules list screen.

Configure the order in which the rules are applied. The MSA filters all email messages according to each rule until a content violation triggers an action (such as delete or quarantine) that prevents further scanning. Change the order of these rules to optimize Data Loss Prevention.

Navigation Path: Security Settings > {MSA} > Configure > Data Loss Prevention > Reorder

To change the order of the DLP rules:

1. Click **Security Settings > {MSA} > Configure > Data Loss Prevention** to open the Data Loss Prevention screen.
2. Select a single rule to reorder.

Tip: You can reorder only one rule at a time.

3. In the upper or lower action bar, click **Reorder**. In the Priority column, an input box appears around the order number of the rule, as shown in [Figure 9-14](#).

Data Loss Prevention

☐ Enable real-time Data Loss Prevention

Rows per page: All

Add Remove **Reorder** Import Export 1 - 6 of 6 Page 1 of 1

☐	Rule	Action	Priority	Enabled
☐	Visa Card card number [A-Z]+	Quarantine entire message	1	☐
☐	MasterCard card number [A-Z]+	Quarantine entire message	2	☐
☒	American Express card number [A-Z]+	Quarantine entire message	3	☐
☐	Diners Club/Carte Blanche card number [A-Z]+	Quarantine entire message	4	☐
☐	Membership Card No. [A-Z]+	Quarantine entire message	5	☐
☐	Bubbly	Quarantine message part	6	☐

Add Remove Reorder Import Export 1 - 6 of 6 Page 1 of 1

Save Reorder Cancel

FIGURE 9-14. Data Loss Prevention rule selected for reordering

- In the Priority column box, delete the existing order number and type a new one.

Note: Be sure to enter a number no larger than the total number of rules in the list. If you enter a number higher than the total number of rules, Data Loss Prevention disregards the entry and does not change the order of the rule.

- Click **Save Reorder**. The rule moves to the priority level that you entered, and all the other rule order numbers change accordingly.

For example, if you select rule number 5 and change it to rule number 3, then rules number 1 and 2 remain the same, and rules numbered 3 and higher increase by one number.

Attachment Blocking

Navigation Path: Security Settings > {MSA} > Configure > Attachment Blocking

Attachment blocking prevents attachments in email messages being delivered to the Microsoft Exchange Information Store. Configure the MSA to block attachments according to the attachment type or attachment name and then *replace*, *quarantine*, or *delete* all the messages that have attachments that match the criteria.

Blocking can occur during Real-time, Manual, and Scheduled Scanning, but the *delete* and *quarantine* actions are not available for Manual and Scheduled Scans.

The extension of an attachment identifies the file type, for example .txt, .exe, or .dll. However, the MSA examines the file header rather than the file name to ascertain the actual file type. Many virus/malware are closely associated with certain types of files. By configuring the MSA to block according to file type, you can decrease the security risk to your Microsoft Exchange servers from those types of files. Similarly, specific attacks are often associated with a specific file name.

Tip: Using blocking is an effective way to control virus outbreaks. You can temporarily quarantine all high-risk file types or those with a specific name associated with a known virus/malware. Later, when you have more time, you can examine the quarantine folder and take action against infected files.

Selecting Blocking Targets

Block attachments with two general strategies: either block all attachments and then exclude specified attachments or specify all the attachments to block.

- **All attachments:** The MSA can block all email messages that contain attachments. However, this type of scan requires a lot of processing. Refine this type of scan by selecting attachment types or names to exclude.
- **Specific attachments:** When you select this type of scan, the MSA only scans for email messages containing attachments that you identify. This type of scan can be very exclusive and is ideal for detecting email messages containing attachments that you suspect contain threats. This scan runs very quickly when you specify a relatively small amount of attachment names or types.

You can block attachments according to:

- **Attachment names:** By default, the MSA examines the file header rather than the file name to ascertain the actual file type. When you set Attachment Blocking to scan for specific names, the MSA will detect attachment types according to their name.
- **Attachment type:** The MSA examines the file header rather than the file name to ascertain the actual file type.

Attachment Blocking Actions

You can configure the MSA to take action against email messages containing detected threats. The following table lists the actions the MSA can take.

TABLE 9-14. Attachment Blocking Actions

ACTION	DESCRIPTION
Replace with text/file	The MSA deletes the attachment and replaces it with a text 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.
Quarantine entire message	Moves the email message that contains the attachment to a folder with restricted access. This action is not available for Manual or Scheduled Scans.
Quarantine message part	Quarantines only the filtered content to the quarantine directory and the recipient receives the message without this content.
Delete entire message	During Real-time Scanning, the MSA deletes the entire email message.

Configuring Attachment Blocking

Navigation Path: Security Settings > {MSA} > Configure > Attachment Blocking

Configuring attachment blocking options for Microsoft Exchange servers involves setting the rules to block messages with certain attachments.

FIGURE 9-15. Attachment Blocking screen

To block attachments:

1. From the **Target** tab on the **Attachment Blocking** screen, update the following as required:
 - **All attachments**
 - **Attachment types to exclude**
 - **Attachment names to exclude**
 - **Specific attachments**
 - **Attachment types**
 - **Attachment names**
 - **Block attachment types or names within ZIP files**
2. From the **Action** tab, update the following as required:
 - **Select an action:** See Table 9-14 on page 9-88.

- **Notifications:** Configure whom to notify about the restriction. Exclude external recipients or senders if required.
 - **Replacement Settings:** Configure the text and file for replacement text. If the action is replace with text/file, WFBS will replace the threat with this text string and file.
3. Click **Save**.

Real-time Monitor

Navigation Path: Security Settings > {MSA} > Configure > Real-time Monitor {upper right of screen}

or

Navigation Path: Windows Start Menu > All Programs > Trend Micro Messaging Security Agent > Real-time Monitor

The Real-time Monitor displays current information about the selected Exchange Server and its Messaging Security Agent (MSA). It shows information about scanned messages and protection statistics, including the number of viruses and spam found, attachments blocked, and content violations.

The Messaging Security Agent **has been running since** field helps you verify whether the MSA is working properly.

To clear old information and start collecting fresh information in real time:

- Click **Reset** to reset the protection statistics to zero.
- Click **Clear Content** to clear older information about scanned messages.

To access the Real-time Monitor:

1. Click **Security Settings**.
2. Select an MSA.
3. Click **Configure**.
4. Click the **Real-time Monitor** link on the upper right portion of the screen.

Web Reputation

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

Web reputation helps ensure that the pages that users access are safe and free from Web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information.

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, Web threat creators constantly change the version or variant used. Because the Web threat is in a fixed location of a website rather than on an infected computer, the Web threat creator constantly modifies its code to avoid detection.

Web reputation blocks Web pages based on their reputation ratings. It queries Trend Micro servers for these ratings, which are correlated from multiple sources, including Web page links, domain and IP address relationships, spam sources, and links in spam messages. By obtaining ratings online, Web reputation uses the latest available information to block harmful pages.

Web reputation helps deter users from following malicious URLs when the feature is enabled. Web reputation queries Trend Micro servers for the reputation rating when an email message with a URL in the message body is received. Depending on the configuration, Web reputation can quarantine, delete, or tag the email message with URLs.

Tip: To save network bandwidth, Trend Micro recommends adding the enterprise internal websites to the Web reputation approved URL list.

Web Reputation Target Settings

A brief description of the options available on the Target tab is available below.

- **Enable Web Reputation:** Select to enable this feature.
- **High:** Select to block a greater number of Web threats but increase the risk of false positives.

- **Medium:** Select to block most Web threats while keeping the false positive count low.
- **Low:** Select to block fewer Web threats but reduce the risk of false positives.
- <http://reclassify.wrs.trendmicro.com>: Click to open a new page to notify Trend Micro of an incorrectly classified URL. You can also use this portal to check the reputation of a website.
- **Enable approved URL list:** Select to use a custom list of approved URLs.
- **Enter approved URL:** Type a URL.
- **Add:** Click to add the URL to the list.
- **Import:** Click to import a URL list.
- **Export:** Click to export the URL list.
- **Approved URL:** Click to sort in ascending or descending order.
- **Save:** Click to save your settings.
- **Restore Defaults:** Click to revert to default settings.

Web Reputation Action Settings

A brief description of the options available on the Action tab is available below.

- **Enable Web Reputation:** Select to enable this feature.
- **Quarantine message to user's spam folder:** Select to deliver the message to the user's junk email folder.
- **Delete entire message:** Select to delete the entire message when ScanMail detects a suspicious URL.
- **Tag and deliver:** Select to specify a tag for the message before delivering when ScanMail detects suspicious URLs.
- **Take action on URLs that have not been assessed by Trend Micro:** Select to treat URLs that have not been classified as suspicious URLs and perform the specified action.
- **Notify:** Select to send a notification.
- **Do not notify:** Select to not send a notification.
- **Save:** Click to save your settings
- **Restore Defaults:** Click to revert to default settings.

Configuring Web Reputation Settings

To configure Web reputation settings:

1. Log on to the Web Console.
2. Click **Security Settings** > {MSA} > **Configure** > **Web Reputation**. The Web Reputation screen displays.
3. Click the **Target** or **Action** tab.
4. Make any necessary changes.
5. Click **Save**.

Messaging Agent Quarantine

When MSAs detect a threat, spam, restricted attachment and/or restricted content in email messages, the Agent can move the message to a quarantine folder. This process acts as an alternative to message/attachment deletion and prevents users from opening the infected message and spreading the threat.

The default quarantine folder on the Message Security Agent is:

```
C:\Program Files\Trend Micro\Messaging Security Client\storage\quarantine
```

Quarantined files are encrypted for added security. To open an encrypted file, use the Restore Encrypted Virus (VSEncode.exe) tool. See [Restoring an Encrypted Virus](#) on page B-12.

Administrators can query the quarantine database to gather information about quarantined messages.

Use Quarantine to:

- Eliminate the chance of important messages being permanently deleted, if they are erroneously detected by aggressive filters
- Review messages that trigger content filters to determine the severity of the policy infraction

- Maintain evidence of an employee's possible misuse of the company's messaging system

Note: Do not confuse the quarantine folder with the end user's spam folder. The quarantine folder is a file-based folder. Whenever an MSA quarantines an email message, it sends the message to the quarantine folder. The end user's spam folder is located in the Information Store for each user's mailbox. The end user's spam folder only receives email messages resulting from an anti-spam quarantine to a user's spam folder and not quarantine actions as the result of content filtering, antivirus/anti-spyware, or attachment blocking policies.

Quarantine Directories

The MSA quarantines email messages according to configured actions. There are four quarantine directories in WFBS:

- **Antivirus:** Quarantines email messages containing virus/malware, spyware/grayware, worms, Trojans, and other malicious threats.
- **Anti-spam:** Quarantines spam and phishing email.
- **Attachment blocking:** Quarantines email messages containing restricted attachments.
- **Content filtering:** Quarantines email messages containing restricted content.

Configuring Quarantine Directories

Configure the quarantine directories on the Microsoft Exchange Server. The quarantine directory will be excluded from scanning.

Note: Quarantine directories are file-based and do not reside on the Information Store.

Navigation Path: Security Settings > {MSA} > Configure > Quarantine > Directory

Quarantine Directory 	
Specify the quarantine directories on the Exchange Server. The quarantine directory will be excluded from scanning.	
Note: Changing the directory will result in the files remaining in the old directory being subject to scanning.	
Antivirus	
Quarantine directory:	E:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine Specify a local path. (For example, C:\Program Files\Trend Micro\Messaging Security Agent\Storage\Quarantine)
Anti-spam Filtering	
Quarantine directory:	E:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine Specify a local path. (For example, C:\Program Files\Trend Micro\Messaging Security Agent\Storage\Quarantine)
Content Filtering	
Quarantine directory:	E:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine Specify a local path. (For example, C:\Program Files\Trend Micro\Messaging Security Agent\Storage\Quarantine)
Attachment Blocking	
Quarantine directory:	E:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine Specify a local path. (For example, C:\Program Files\Trend Micro\Messaging Security Agent\Storage\Quarantine)
Save	

FIGURE 9-16. Quarantine Directory screen

To set up the Quarantine Directory

- From the **Quarantine Directory** screen, set the directory path for the following quarantine folders:
 - Antivirus**
 - Anti-Spam**
 - Content Filtering**
 - Attachment Blocking**
 See [Quarantine Directories](#) on page 9-94.
- Click **Save**.

Agent Quarantine Folder

Whenever an Agent detects an Internet threat in a file and the scan action for that type of threat is quarantine, the Agent encrypts the infected file, moves it to the Client's quarantine folder, and sends it to the Trend Micro Security Server quarantine folder. Worry-Free Business Security encrypts the infected file to prevent it from infecting other files.

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

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

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

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

If the Agent is unable to send the encrypted file to the Trend Micro Security Server for any reason, such as network connection problems, the encrypted file remains in the Client's quarantine folder. The Agent attempts to resend the file when it reconnects to the Trend Micro Security Server.

For more information on configuring scan settings or changing the location of the quarantine folder, see [Virus Scan Settings](#) on page 11-8.

Querying Quarantine Directories

To view information about quarantined messages, query the Quarantine Directories.

Navigation Path: Security Settings > {MSA} > Configure > Quarantine > Query

Quarantine Query ?

Query the quarantine database.

Date/Time Range

From: 12/18/2007 12 : 40

To: 12/19/2007 12 : 40

Reasons Quarantined

☒ All reasons

☐ Specified types

☐ Virus scan

☐ Anti-Spam

☐ Content filtering

☐ Attachment blocking

☐ Unscannable message parts

Resend Status

☒ Never been resent

☐ Resent at least once

☐ Both of the above

Advanced Criteria

Sender:

Recipient:

Subject:

Sort by: Scan time ☐ Ascending ☒ Descending

Display: 15 per page

FIGURE 9-17. Quarantine Query screen

To query the Quarantine Directories:

- From the **Quarantine Query** screen, update the following as required:
 - Date/Time Range**
 - From Date and Time**
 - To Date and Time**

- **Reasons Quarantined**
 - **All Reasons**
 - **Specified Types:** Select from Virus scan, Anti-Spam, Content filtering, Attachment blocking, and/or Unscannable message parts.
- **Resend Status**
 - **Never been resent**
 - **Resent at least once**
 - **Both of the above**
- **Advanced Criteria**
 - **Sender:** Messages from specific senders. Use wildcards if required.
 - **Recipient:** Messages from specific recipients. Use wildcards if required.
 - **Subject:** Messages with specific subjects. Use wildcards if required.
 - **Sort by:** Configure the sort condition for the results page.
 - **Display:** Number of results per page.

2. Click **Search**. See [Quarantined Messages](#) on page 9-98.

Quarantined Messages

After running a query, view the details of the message and determine its safety. If you feel a message is safe, resend the message to the original recipients. If you feel otherwise, delete the message. See [Querying Quarantine Directories](#) on page 9-97.

WARNING! The quarantine folder contains email messages that have a high-risk of being infected. Be cautious when handling email messages from the quarantine folder so that you do not accidentally infect the client.

Quarantine Query			
Query the quarantine database.			
Results from 12/19/2007 13:27:00 to 12/20/2007 13:27:00			
 Resend  Delete			
☐	Scan time▼	Sender	Recipient
☐	12/19/2007 17:40:56	Robert.Chin@ejgallo.com;	Spam@trendmicro.com;
☐	12/19/2007 17:40:56	bg3@hew.com;	bg3@hew.com;
☐	12/19/2007 17:40:56	Mildred.Ling@VerizonWireless.com;	Spam@TrendMicro.com;
		~5rg@sfn11.com;	~5?@adm.uned.es;

FIGURE 9-18. Quarantine Query Results screen

The **Quarantine Query Results** screen displays the following information about the messages:

- **Scan time**
- **Sender**
- **Recipient**
- **Subject**
- **Reason:** The reason the email message is quarantined.
- **File name:** Name of the blocked file in the email message.
- **Quarantine path:** The quarantined location of the email message. Administrator's can decrypt the file using `VSEncoder.exe` (See [Restoring an Encrypted Virus](#) on page B-12) and then rename it to `.eml` to view it.

WARNING! Viewing infected files could spread the infection.

- **Resend status**

To resend a quarantined message:

From the **Quarantine Query Results** screen, select the message and click .

The message is re-sent to the original recipients.

Note: If you resend a quarantined message that was originally sent using Microsoft Outlook, the recipient may receive multiple copies of the same message. This may occur because the Virus Scan engine strips each message that it scans into several sections.

Maintaining Quarantine Directories

Navigation Path: Security Settings > {MSA} > Configure > Quarantine > Maintenance

Use this feature to manually or automatically delete quarantined messages. This feature can delete all messages, messages that have been resent, messages that have not been resent.



FIGURE 9-19. Quarantine Maintenance screen

To maintain Quarantine Directories:

1. From the **Quarantine Maintenance** screen, update the following as required:
 - **Enable automatic maintenance:** Only available for automatic maintenance.
 - **Files to delete**
 - All quarantined files
 - Quarantined files that have never been resent
 - Quarantined files that have been resent at least once

- **Action:** The number of days the messages should be stored. For example, if the date is November 21 and you typed 10 in **Delete selected files older than**, then the MSA deletes all files from before November 11 when it performs the automatic delete.

2. Click **Save**.

Managing the End User Quarantine Tool

During installation, the MSA adds a folder, **Spam Mail**, to the server-side mailbox of each end user. When spam messages arrive, the system quarantines them in this folder according to spam filter rules predefined by the MSA. End users can view this spam folder to open, read, or delete the suspect email messages. See [Spam Maintenance](#) on page 9-105.

Client-side Spam Mail Folder

End users can open email messages quarantined in the spam folder. When they open one of these messages, two buttons appear on the actual email message: **Approved Sender** and **View Approved Sender List**.

- When an end user opens an email message from the Spam Mail folder and clicks **Approved Sender**, then the sender's address for that email is added to the end user's Approved Senders list.
- Clicking **View Approved Sender List** opens another screen which allows the end user to view and modify their list of approved senders by email address or domain.

Approve Senders

When the end user receives an email message in the Spam Mail folder and clicks **Approve Sender**, the MSA moves the message to the end users local inbox and adds the sender's address to the end user's personal Approved Sender List. The MSA logs the event.

When the Microsoft Exchange server receives messages from the addresses on the end user's Approved Senders list, it delivers them to the end user's inbox, regardless of the header or content of the message.

Note: Note: The MSA also provides administrators with an Approved Senders and Blocked Senders list. The MSA applies the administrator's approved senders and blocked senders before considering the end user list.

End User Quarantine Housekeeping Feature

The MSA housekeeping feature performs the following tasks every 24 hours at the default time of 2:30 AM:

- Auto-deletes expired spam messages
- Recreates the spam folder if it has been deleted
- Creates spam folders for newly created mail accounts
- Maintains email message rules

The housekeeping feature is an integral part of the MSA and requires no configuration.

Operations

During installation, the Messaging Security Agent (MSA) adds a folder, **Spam Mail**, to the server-side mailbox of each end user. When spam messages arrive, the system quarantines them in this folder according to spam filter rules predefined by MSA. End users can view this spam folder to open, read, or delete the suspect email messages.

Alternatively, Administrators can create the Spam Mail folder on Microsoft Exchange. When an Administrator creates a mailbox account, the mailbox entity will not be created immediately in Microsoft Exchange server, but will be created under the following conditions:

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

The Administrator must first create the mailbox entity before EUQ can create the Spam Folder.

End users can open email messages quarantined in the spam folder. When they open one of these messages, two buttons appear on the email message: **Approve Sender** and **View Approved Sender List**. When they click **Approve Sender**, the MSA moves the message from the spam folder to their local inbox, adds the address of the message to their personal Approved Sender List and logs an entry of the event (the Administrator can view this log in a report at a later time). Clicking **View Approved Sender List** opens another screen which allows the end user to view and modify their list of approved senders by name, SMTP email address, or domain. When the Microsoft Exchange server receives messages from the addresses on the end user's approved sender list, it delivers them to the end user's inbox, regardless of the header or content of the message.

Notification Settings

Navigation Path: Security Settings > {MSA} > Configure > Operations > Notification Settings

WFBS can send notifications in the form of email messages to various alerts. Some notifications can be configured to apply to only internal email messages. Define the email addresses or domains to treat as internal addresses. Custom Internal Email Definitions are useful if your company has two or more domains and you would like to treat email messages from both domains as internal email messages. For example, example.com and example.net.

The recipients on your Internal Email Definitions list will receive messages for notifications when you select the **Do not notify external recipients** check box under the Notification settings for **Antivirus**, **Content Filtering**, and **Attachment Blocking**. Do not confuse the Internal Email Definitions list with the Approved Senders list.

To prevent all email from addresses with external domains from being labeled as spam, add the external email addresses to the **Approved Senders** lists for Anti-Spam.

Notification Settings

Administrator Account

Type the email address for the administrator who will send alerts and notifications.

Email address:

For example: user@domain.com

Internal Email Definition

☒ Default (Internal mail: email messages with the same domain.)

☐ Custom internal mail definition [?](#)

Add email addresses or domain names:

FIGURE 9-20. Notification Settings screen

To configure notification settings:

1. From the **Notification Settings** screen, update the following as required:
 - **Email address.** The address on behalf of whom WFBS will send notification messages.
 - **Internal Email Definition**
 - **Default:** WFBS will treat email messages from the same domain as Internal Emails.
 - **Custom:** Specify individual email addresses or domains to treat as internal email messages.
2. Click **Save**.

Spam Maintenance

Navigation Path: Security Settings > {MSA} > Configure > Operations > Spam Maintenance

Spam Maintenance

☒ Enable End User Quarantine tool ⓘ

End User Quarantine Settings

[Create spam folder and delete spam messages](#)

Client Spam Folder Settings Last successful maintenance:

Spam folder name: "Spam Mail"

Delete spam messages older than: 14 days

End User Quarantine tool exception list Last successful maintenance:

Add users who want to have End User Quarantine tool disabled:

Disable the End User Quarantine tool for these users:

FIGURE 9-21. Spam Maintenance screen

To maintain spam:

- From the **Spam Maintenance** screen, update the following as required:
 - Enable End User Quarantine tool:** Creates an end-user quarantine tool for all mailboxes on your Exchange server.

Tip: If you select this option, Trend Micro recommends disabling the Trend Micro Anti-Spam toolbar option on Agents to increase performance on clients.

Note: You must enable the EUQ tool in order for the Anti-spam > quarantine message to user's spam folder action to work.

- **Create spam folder and delete spam messages:** Create a new spam folder for each new user that you add to the Exchange server where you have installed the end user quarantine tool. Clicking **Create spam folder and delete spam messages** immediately creates the spam folder for the new user.
- **Delete spam messages older than:** Specify the number of days to keep spam messages before deleting the messages.
- **End User Quarantine tool exception list:** Email addresses in this list do not have End User Quarantine enabled.

To add a new email address, type the email address and click **Add**.

To delete an existing email address, select the address and click **Delete**.

2. Click **Save**.

Trend Support/Debugger

The Messaging Security Agent (MSA) Debugger can assist you in debugging or just reporting the status of the MSA processes. When you are having unexpected difficulties you can use debugger to create debugger reports and send them to Trend Micro technical support for analysis.

Each Messaging Security module inserts messages into the program, and then records the action into log files upon execution. You can forward the logs to Trend Micro Technical Support staff to help them debug the actual program flow in your environment.

Use the debugger to generate logs on the following modules:

- Messaging Security Agent Master Service
- Messaging Security Agent Remote Configuration Server
- Messaging Security Agent System Watcher
- Virus Scan API (VSAPI)
- Simple Mail Transfer Protocol (SMTP)
- Common Gateway Interface (CGI)

By default, the MSA keeps the logs in the following directory:

```
c:\Program Files\Trend Micro\Messaging Security Agent\Debug
```

View the output with any text editor.

Generating System Debugger Reports

Navigation Path: Security Settings > {MSA} > Configure > Operations > Trend Support/Debugger

Generate debugger reports to assist Trend Support in troubleshooting your problem.

To generate reports using the Debugger:

Trend Support/System Debugger 			
☐	Module Description	Module Name	File Name
☐	Trend Micro Messaging Security Agent Master Service	<SMEX_Master.exe>	SMEX_Master.log, SMEX_Master-yy-mm-dd-xxxxx.log
☐	Trend Micro Messaging Security Agent Remote Configuration Server	<SMEX_RemoteConfig.exe>	SMEX_RemoteConfig.log, SMEX_RemoteConfig-yy-mm-dd-xxxxx.log
☐	Trend Micro Messaging Security Agent System Watcher	<SMEX_SystemWatcher.exe>	SMEX_SystemWatcher.log, SMEX_SystemWatcher-yy-mm-dd-xxxxx.log
☐	Virus Scan API (VSAPI)	<store.exe>	store.log, store-yy-mm-dd-xxxxx.log
☐	Simple Mail Transfer Protocol (SMTP)	<inetinfo.exe>	inetinfo.log, inetinfo-yy-mm-dd-xxxxx.log
☐	Common Gateway Interface (CGI)	<cgDispatcher.exe>	cgDispatcher.log, cgDispatcher-yy-mm-dd-xxxxx.log
Apply			

FIGURE 9-22. Trend Support/System Debugger screen

- From the **Trend Support/System Debugger** screen, select the modules to monitor:
 - Messaging Security Agent **Master Service**
 - Messaging Security Agent **Remote Configuration Server**
 - Messaging Security Agent **System Watcher**
 - Virus Scan API (VSAPI)**
 - Simple Mail Transfer Protocol (SMTP)**
 - Common Gateway Interface (CGI)**
- Click **Apply**. The debugger starts collecting data for the selected modules.

Note: The Messaging Security Agent Debugger continues to collect debug data until you clear all the items marked for debugging and click **Apply**.

Replicating Settings for Microsoft Exchange Servers

To save time and maintain consistent security settings, you can replicate the settings from one Microsoft Exchange server to another.

To replicate settings:

1. From the **Security Settings** screen, choose the Microsoft Exchange server from which you want to replicate settings.
2. Click **Replicate**. The **Security Settings > Replicate** screen opens displaying the source you selected in the previous screen.
3. Select the target Microsoft Exchange server or server group to which you will replicate the settings.
4. Click **Apply**.

Note: You can only replicate settings from a source Microsoft Exchange server to a target Microsoft Exchange server that share the same domain.

Adding a Disclaimer to Outbound Email Messages

You can add a disclaimer message only to outgoing email messages.

To add a disclaimer to each outbound mail:

1. Create a text file and add the disclaimer text to this file.
2. Modify the following keys in the registry:
 - First key:
Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion
Key: EnabledDisclaimer
Type: REG_DWORD
Data value: 0 - Disable, 1 - Enable
 - Second key:

Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail
for Exchange\CurrentVersion

Key: DisclaimerSource

Type: REG_SZ

Value: The full path of the disclaimer content file.

For example, C:\Data\Disclaimer.txt

Note: By default, WFBS will detect if an outbound mail is sent to the internal or external domains, and add a disclaimer to each mail sent to the external domains. The user can overwrite the default setting and add a disclaimer to each outbound mail except the domains included in the following registry key:

- Third key:

Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail
for Exchange\CurrentVersion

Key: InternalDomains

Type: REG_SZ

Value: Type the domain names to exclude. Use a semicolon (;) to separate multiple items.

For example: domain1.org;domain2.org

Note: The domain names here are the DNS names of the Exchange servers.

Configuring Exclusions for Messaging Security Agents

To configure scanning for email messages that are very large or contain very large attachments:

- Click **Message body size exceeds** and type a number. The Messaging Security Agent only scans email messages when the size of the body of the message is smaller or equal to the specified amount.

Trend Micro recommends a 30 MB limit.

- Click **Attachment size exceeds** and type a number. The Messaging Security Agent only scans email messages when the size of the attachment file is smaller than or equal to the specified amount.

Trend Micro recommends a 30 MB limit.

To configure scanning for compressed files:

- Click **Decompressed file count exceeds** and type a number to set a restriction for the amount of decompressed files that the Messaging Security Agent will scan.

When the amount of decompressed files within the compressed file exceeds this number, then the Messaging Security Agent only scans files up to the limit set by this option.

- Click **The size of decompressed files exceeds** and type a number that represents the size limit in MB. The Messaging Security Agent only scans compressed files that are smaller or equal to this size after decompression.
- Click **The number of layers of compression exceed** and type a number from 1-20. The Messaging Security Agent only scans compressed files that have less than or equal to the specified layers of compression.

For example, if you set the limit to 5 layers of compression, then the Messaging Security Agent will scan the first 5 layers of compressed files, but not scan files compressed to 6 or more layers.

- Click **Size of decompressed file is “x” times the size of compressed file** and type a number. The Messaging Security Agent only scans compressed files when the ratio of the size of the decompressed file compared to the size of the compressed file is less than this number.

This function prevents the Messaging Security Agent from scanning a compressed file that might cause a Denial of Service (DoS) attack. A DoS attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing the Messaging Security Agent from scanning files that decompress into very large files helps prevent this problem from happening.

Example: For the table below, the value typed for the “x” value is 100.

FILE SIZE (NOT COMPRESSED)	FILE SIZE (NOT COMPRESSED)	RESULT
500 KB	10 KB (ratio is 50:1)	Scanned
1000 KB	10 KB (ratio is 100:1)	Scanned
1001 KB	10 KB (ratio exceeds 100:1)	Not scanned *
2000 KB	10 KB (ratio is 200:1)	Not scanned *

* The Messaging Security Agent takes the action you configure for excluded files.

Advanced Scan Options for Microsoft Exchange Servers

To further customize your Antivirus scanning options, set one or more of the following Advanced Options.

To decrease scanning time, exclude very large or compressed files from scanning:

1. From the **Antivirus > Target** screen, expand the Exclusions panel.
2. Set up the excluded files.

To scan for Macro viruses:

1. From the **Antivirus > Action** screen, expand the Macros panel.
2. Set macro scanning options.

To set the Messaging Security Agent to take action against Unscannable files:

- Select an action from the drop-down list. The default action is Pass.
The MSA does not support scanning for encrypted or password-protected files.

To set the Messaging Security Agent to take action against Excluded files:

- Select an action from the drop-down list. The default action is Pass.
The Excluded files are set up from the **Antivirus > Target** screen and include very large or compressed files.

To set up the Backup Directory:

- Type a directory path in the space provided or accept the default path that the installation program created.

To customize the Replacement Settings:

- Type the customized information in the space provided.

When the MSA performs the Replace with text/file action against a detected threat, it replaces the original file (or text from an email message) with the content shown in this field.

Advanced Macro Scanning

Advanced macro scanning supplements regular virus/malware scanning. It uses heuristic scanning to detect macro viruses or simply strips all detected macro codes. The Messaging Security Agent takes action against malicious macro code depending on the action that you configure from the Antivirus screen.

Heuristic scanning is an evaluative method of detecting viruses that uses pattern recognition and rules-based technologies to search for malicious macro code. This method excels at detecting undiscovered viruses and threats that do not have a known virus signature.

When the MSA detects a malicious macro code using heuristic scanning, it takes action against the malicious code based on the action that you configured from the Antivirus screen. When you select **Delete all macros detected by advanced macro scanning**, the MSA strips all macro code from the scanned files.

To set the Messaging Security Agent to scan unknown macro viruses:

1. From the **Antivirus > Action** screen, click  to expand the **Macros** panel.
2. Select **Enable advanced macro scan**.
3. Select a detection type:
 - Select **Heuristic level** and set a level for the heuristic rules.
 - Level 1 uses the most specific criteria, but detects the least macro codes.
 - Level 4 detects the most macro codes, but uses the least specific criteria and may falsely identify safe macro code as harboring malicious macro code.

Tip: Trend Micro recommends a heuristic scan level of 2. This level provides a high detection level for unknown macro viruses, fast scanning speed, and it uses only the necessary rules to check for macro virus strings. Level 2 also has a low level of incorrectly identifying malicious code in safe macro code.

- Select **Delete all macros detected by advanced macro scanning** to have the MSA strip all of the macro code that it detects.

4. Click **Save**.

Internal Address Definition

The Messaging Security Agent (MSA) divides email traffic into two network categories: internal and external. The MSA queries the Microsoft Exchange server to learn how the internal and external addresses are defined. All internal addresses share a common domain and all external addresses do not belong to that domain.

For example, if the internal domain address is “@trend_1.com”, then the MSA classifies addresses such as “abc@trend_1.com” and “xyz@trend_1.com” as internal addresses. The MSA classifies all other addresses, such as “abc@trend_2.com” and “jondoe@123.com” as external.



Chapter 10

Using Outbreak Defense

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

The topics discussed in this chapter include:

- *Outbreak Defense Strategy* on page 10-2
- *Outbreak Defense Current Status* on page 10-4
- *Potential Threat* on page 10-8
- *Configuring Vulnerability Assessment Settings* on page 10-16
- *Viewing Automatic Outbreak Defense Details* on page 10-18

Outbreak Defense Strategy

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

WFBS initiates Outbreak Defense in response to instructions that it receives in the Outbreak Prevention Policy. The Trend Micro Outbreak Prevention Policy is designed and issued by Trend Micro to give optimal protection to your clients and network during outbreak conditions. Trend Micro issues the Outbreak Prevention Policy when it observes frequent and severe virus/malware incidents that are actively circulating on the Internet.

By default, the Security Server downloads the Outbreak Prevention Policy from the Trend Micro ActiveUpdate Server every 30 minutes or whenever the Security Server starts up.

During Outbreak Defense, the Security Server enacts the Outbreak Defense Policy and takes action to protect your clients and network. At such a time, the normal functions of your network will be interrupted by measures like blocked ports and inaccessible directories. You can use the Outbreak Defense Settings to customize the Outbreak Defense for your clients and network, thus avoiding unexpected consequences from the policies enacted during Outbreak Defense.

Trend Micro may send out Red or Yellow alerts and issue responses similar to the following:

Red Alerts

Several business units may have reported a rapidly spreading virus/malware. As a response, Trend Micro may trigger its 45-minute Red Alert solution process, which involves releasing preventive solutions and scan patterns and sending out relevant notifications. Trend Micro may also send out fix tools and information regarding related vulnerabilities and threats.

Yellow Alerts

Infection reports may be received from several business units as well as support calls confirming scattered instances. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download. In case of an email-spreading

virus/malware (Advanced only), content filtering rules, called Outbreak Prevention Policies (OPP), are sent out to automatically block related attachments on servers equipped with the product functionality.

Outbreak Life Cycle

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

TABLE 10-1. Outbreak Defense Response to the Outbreak Life Cycle Stages

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

Outbreak Defense Actions

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

- Blocking shared folders to help prevent virus/malware from infecting files in shared folders
- Blocking file with certain extensions on the Microsoft Exchange Server (Advanced only)
- Adding content filtering rules to the Messaging Security Agent (Advanced only)
- Blocking ports to help prevent virus/malware from using vulnerable ports to spread the infection on the network and clients

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

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

Outbreak Defense Current Status

Navigation Path: Outbreak Defense > Current Status

The Web Console displays and tracks the status of a world-wide virus/malware outbreak threat on the **Current Status** screen. The status roughly corresponds to the outbreak life cycle.

During an outbreak, Outbreak Defense uses the Outbreak Defense Strategy to protect your computers and networks. In each stage, it refreshes the information in the Current Status page. The three stages of Outbreak Defense:

1. Threat Prevention
2. Threat Protection
3. Threat Cleanup

Threat Prevention

The Threat Prevention stage of the **Current Status** screen displays information about recent threats, clients that have alerts enabled, and clients that are vulnerable to the current threat.

Threat Information

The Threat Information section displays information about virus/malware that are currently on the Internet and could potentially affect your network and clients. Based on Threat Information, the Outbreak Prevention Policy takes steps to protect the network and clients while Trend Micro develops a solution (See [Outbreak Prevention Policy](#) on page D-2). Learn more about a threat by clicking **Help > Security Info** to go to the Trend Micro website.

This section provides the following information:

- **Risk Level:** The level of risk the threat poses to clients and networks based on the number and severity of virus/malware incident.
- **Automatic Response Details:** Click to view the specific actions Outbreak Defense is using to protect your clients from the current threat. Click **Disable** to stop the Automatic Response from the server-side and Agents.

Alert Status for Online Computers

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

Vulnerable Computers

The Vulnerable Computers section displays a list of clients that have vulnerabilities that make them susceptible to the threat displayed in the Threat Information section.

Threat Protection

The Threat Protection stage of the **Current Status** screen provides information about the Solution Download Status in regard to Trend Micro update components and the Solution Deployment Status in regard to all Agents.

Solution Download Status

Displays a list of components that need to be updated in response to the threat listed in the Threat Information section.

Solution Deployment Status

Displays the number of Agents that have updated and outdated components. It also provides links to view the clients with updated or outdated components.

Threat Cleanup

The Threat Cleanup stage of the **Current Status** screen displays the status of the scan that takes place after the updated components have been deployed. The Threat Cleanup stage also displays the status of clients after the scan and lists whether the updates were successful in cleaning or removing threat remnants.

Note: For a scan to automatically take place after the new components have been deployed, it has to be enabled in the **Outbreak Defense > Settings** screen.

Computer Scanning Status For

Click the links to display a list of clients that have either received notification to scan for threats or have yet to receive notification. Clients that are not turned on or that have been disconnected from the network cannot receive notifications.

Computer Cleanup Status For

This panel displays the results of the Cleanup scan. Click **Export**, to export this information.

Vulnerability Assessment

Vulnerability Assessment provides system administrators or other network security personnel with the ability to assess security risks to their networks. The information they generate by using Vulnerability Assessment gives them a clear guide as to how to resolve known vulnerabilities and secure their networks.

Use Vulnerability Assessment to:

- Scan computers on your network for vulnerabilities.
- Identify vulnerabilities according to standard naming conventions. Find out more about the vulnerability and how to resolve it by clicking on the vulnerability name.
- Display the vulnerabilities by computer and IP address. Results include the risk level that the vulnerabilities represent to the computer and to the entire network.
- Report vulnerabilities according to individual computers and describe the security risks those computers present to the overall network.
- Configure tasks that scan any or all computers attached to a network. Scans can search for single vulnerabilities or a list of all known vulnerabilities.
- Run manual assessment tasks or set tasks to run according to a schedule.
- Request blocking for computers that present an unacceptable level of risk to network security.
- Create reports that identify vulnerabilities according to individual computers and describe the security risks those computers present to the overall network. The reports identify the vulnerability according to standard naming conventions so that Administrators can research further to resolve the vulnerabilities and secure the network.
- View assessment histories and compare reports to better understand the vulnerabilities and the changing risk factors to network security.

Vulnerability Assessment Pattern File

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

Potential Threat

Navigation Path: Outbreak Defense > Potential Threat

The **Potential Threat** screen displays information about security risks to your clients and network. The Security Server gathers threat information by running Vulnerability Assessment and Cleanup Services to clean threats.

Outbreak Defense > Potential Threat

As part of the ongoing health of your network, Trend Micro catches any vulnerable computers and provide you with a list of computers that you must manually clean to remove threats. Below you will find a list of computers that require your attention.

Vulnerable Computer(s) 02/13/2007 21:05:10

Your network has the following vulnerabilities that WORM_SASSER.B exploits. To ensure the security of your network, please follow the instruction and take necessary actions.

[Export](#) [Scan for Vulnerability Now](#) Total: 10 records Page: 35 1 of 2

Risk Level	Computer	IP Address	Computer Group	# of Vulnerabilities
Highly Critical	Desktop US	1.0.333.0	Desktops (default)	090
Critical	Server TW Taipei 101	90.222.223.700	Desktop (default)	999
Important	Desktop-49	111.222.033.4	Desktops (default)	5643575375
Moderate	Server TW Taipei 101	111.292.333.440	Desktops (default)	6573575
Low	Server TW Taipei 101	0.222.333.994	Desktops (default)	66

Highly Critical Critical Important Moderate Low

Computer(s) to Cleanup 07/03/2007 21:46:17

Client/Server/Messaging Security for SMB has tried to cleanup the computers with the latest pattern. Please see the results below. To manually cleanup using the new components, click Cleanup Now.

[Export](#) [Cleanup Now](#) Total: 10 records Page: 25 1 of 2

Computer	Date/Time	IP Address	Computer Group	Threat Name	Action Performed
Desktop1771	05/06/2005 hh:mm:ss	1.0.333.0	Desktops (default)	WORM_SASSER.B	090
Desktop21	05/06/2005 hh:mm:ss	90.222.223.700	Desktop (default)	WORM_SASSER.B	999
Desktop221	05/06/2005 hh:mm:ss	111.222.033.4	Desktops (default)	Never caught virus	5643575375
Desktop21	05/06/2005 hh:mm:ss	111.292.333.440	Desktops (default)	Super Virus	6573575
Desktop661	05/06/2005 hh:mm:ss	0.222.333.994	Desktops (default)	Uncatched virus	66

FIGURE 10-1. Potential Threat screen

Unlike the **Current Threat** screen that only displays information about a current threat, the **Potential Threat** screen displays information about all the threats to your clients and network that have not been resolved.

Vulnerable Computers

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.

The Vulnerable Computers section lists all the clients on your network that have vulnerabilities discovered since the last vulnerability assessment. You can view the Last updated time in the top-right hand corner of the screen.

The **Potential Threat** screen ranks the clients according to the risk level that they pose to the network. Risk level is calculated by Trend Micro and represents the relative number and severity of vulnerabilities for each client.

When you click **Scan for Vulnerabilities Now**, WFBS runs a Vulnerability Assessment. A Vulnerability Assessment checks all the clients on your network for vulnerabilities and displays the results in the **Potential Threat** screen. Vulnerability Assessments can provide the following information about clients on your network:

- Identify vulnerabilities according to standard naming conventions. Find out more about the vulnerability and how to resolve it by clicking on the vulnerability name.
- Display the vulnerabilities by client and IP address. Results include the risk level that the vulnerabilities represent to the client and to the entire network.
- Report vulnerabilities. Report vulnerabilities according to individual clients and describe the security risks those clients present to the overall network.

Computers to Cleanup

Cleanup runs in the background whenever Agents run Antivirus scans. You do not need to set up scheduled Cleanup scans.

Security Agents use Cleanup to protect clients against Trojan horse programs (or Trojans). To address the threats and nuisances posed by Trojans and other malware, Cleanup does the following:

- Detects and removes live Trojans and other malware applications
- Kills processes that Trojans and other malware applications create
- Repairs system files that Trojans and other malware modify
- Deletes files and applications that Trojans and other malware create

To accomplish these tasks, Cleanup makes use of these components:

- **Damage Cleanup Engine:** The engine Cleanup uses to scan for and remove Trojans and Trojan processes, worms, and spyware.
- **Virus Cleanup Pattern:** Used by the Damage Cleanup Engine. This template helps identify Trojans and Trojan processes, worms, and spyware, so the Damage Cleanup Engine can eliminate them.

Cleanup runs on clients on these occasions:

- Users perform a manual cleanup from the Agent
- Users run a Manual Scan or Clean
- After hot fix or patch deployment
- When the Security Server starts

Because Cleanup runs automatically, you do not need to configure it. Users are not even aware when it is executed because it runs in the background (when Agents are running). However, the Security Server may sometimes notify the user to restart their computer to complete the cleanup.

Configuring Outbreak Defense Settings

Navigation Path: Outbreak Defense > Settings > Vulnerability Assessment

Use the Settings screen to configure Outbreak Defense and Vulnerability Assessment options.

Note: Trend Micro designed Outbreak Defense defaults to provide optimal protection for your clients and network. Before customizing your Outbreak Defense settings, carefully consider the settings and only modify them when you understand the consequences.

Outbreak Defense > Settings 

Set up your response to vulnerabilities and outbreaks for the entire network.

Outbreak Defense

Vulnerability Assessment

Automatic Outbreak Defense

☒ Enable Automatic Outbreak Defense for Red Alerts issued by Trend Micro  
Disable Red Alerts after: days
☒ Disable Red Alerts after required component(s) deployed.
Perform automatic virus scan after required component(s) deployed for:
☐ Desktops/Servers
☐ Exchange server
☐ Enable Automatic Outbreak Defense for Yellow Alerts issued by Trend Micro  
Disable Yellow Alerts after: days
☐ Disable Yellow Alerts after required pattern/engine deployed.
Perform automatic virus scan after required component(s) deployed for:
☐ Desktops/Servers
☐ Exchange server

Exceptions

Scheduled Policy Download Settings

FIGURE 10-2. Outbreak Defense tab of Outbreak Defense Settings screen

To configure the Outbreak Defense settings:

- Update the following options as required:
 - Enable Outbreak Defense for Red Alerts issued by Trend Micro:** Outbreak Defense policies stay in effect until you click **Outbreak Defense > Current Status > Disable** or one of the disable settings are met. When the Security Server downloads a new Outbreak Prevention Policy, the old policy stops.
 - Disable Red Alerts after x days:** The duration for the Outbreak Defense alert.
 - Perform automatic virus scan after required components deployed for:
 - Desktops/Servers
 - Exchange servers (Advanced only)
 - Yellow Alert settings:** Configure the options for Yellow Alerts. See [Yellow Alerts](#) on page 10-2.

- **Exceptions:** The ports that will not be blocked during Outbreak Defense Automatic Response. See [Outbreak Defense Exceptions](#) on page 10-14.

Note: When adding a new exception, ensure to select **Enable this exception**.

- **Scheduled Policy Download Settings:** The settings for periodically downloading updated components.
 - Frequency
 - **Source:** The source of the updates.
 - **Trend Micro ActiveUpdate server** (default)
 - **Intranet location containing a copy of the current file**
 - **Other update source:** Any other update source on the Web.

2. Click **Save**.

Recommended Outbreak Defense Settings

The following settings are provided for optimal protection:

TABLE 10-2. Recommended Outbreak Defense Settings

SETTING	RECOMMENDED VALUE
Enable Automatic Outbreak Defense for Red Alerts issued by Trend Micro	Enabled
Disable Red Alerts after	2 days
Disable Red Alerts after required components deployed	Enabled
Automatic Desktop/Server scans	Enabled
Automatic Microsoft Exchange scans (Advanced only)	Enabled
Enable Automatic Outbreak Defense for Yellow Alerts issued by Trend Micro	Disabled
Disable Yellow Alerts after	NA

TABLE 10-2. Recommended Outbreak Defense Settings (Continued)

SETTING	RECOMMENDED VALUE
Disable Yellow Alerts after required pattern/engine deployed	NA
Disable Yellow Alerts after required pattern/engine deployed.	NA
Automatic Desktop/Server scans	Enabled
Automatic Microsoft Exchange scans (Advanced only)	Enabled
Exceptions	Ports for the following services will not be blocked during Outbreak Defense Automatic Response: DNS NetBios HTTPS (Secure Web server) HTTP (Web server) Telnet SMTP (Simple mail protocol) FTP (File transfer protocol) Internet Mail (POP3)
Scheduled Policy Download Settings	Frequency: Every 30 minutes Source: Trend Micro ActiveUpdate Server

Outbreak Defense Exceptions

Navigation Path: Outbreak Defense > Settings > Exception

During Outbreak Defense, the Security Server might block ports to prevent threats from accessing the computers on your network. However, you might have ports that you always want to keep open to ensure communication between the Security Server and other computers and applications. You can add these ports to the exclusion list so that they will never be blocked even during Outbreak Defense.

WARNING! **WARNING!** Trend Micro designed Outbreak Defense to block ports most commonly used by attackers and malicious software. Adding exceptions to port blocking might leave your computers and networks vulnerable.

☐	Description	Protocol	Port	Enabled
☐	Web service (HTTP)		80	✓
☐	Send mail (SMTP)		25	✓
☐	Internet mail (POP3)		110	✗
☐	File transfer (FTP)		20-21	✓
☐	Telnet		23	✗

FIGURE 10-3. Exceptions section of Outbreak Defense Settings screen

To add an exception:

1. Click the plus (+) icon for the **Exceptions** section.
2. Click **Add**.
3. From the **Outbreak Defense > Settings > Add Exception** screen, update the following options as required:
 - **Enable this exception**
 - **Description**
 - **Protocol**
 - Transmission Control Protocol (TCP)
 - User Datagram Protocol (UDP)

- Internet Control Message Protocol (ICMP).
- **Ports:** Type a port range or individual ports for the exception. Separate multiple entries with semicolons (;).

4. Click **Add**.

To edit an exception:

1. From the Edit Exceptions screen, select **Enable this exception**.
2. Type a description for your exception in the **Description** field.
3. From the Protocol drop-down list, select the communication method that you want to exclude. You can select:
 - **Transmission Control Protocol (TCP)**
 - **User Datagram Protocol (UDP)**
 - **Internet Control Message Protocol (ICMP).**
4. Enter the ports to exclude.
 - For a range of ports, select **Port range** and then enter the first number in the range and then the last.
 - To exclude specific ports, select **Specified ports** and enter the specific port numbers.
5. Click **Save**.

To remove an exception:

Tip: Disable an Exception instead of removing it.

1. Click the plus (+) icon for the **Exceptions** section.
2. Select the exception and click **Remove**.
3. Click **OK** to confirm.

Removing Ports from the Exceptions List

To remove a port from the exception list:

1. On the main menu, click **Outbreak Defense > Settings**. The Outbreak Defense > Settings screen appears with the Outbreak Defense tab selected by default.
2. Click next to the **Exceptions**. The Exception section expands to display a list of ports to exclude from blocking.
3. Select a port to remove, and click the **Remove** icon.
4. Click **OK** on the confirmation prompt. This removes the port from the exception list.

Configuring Vulnerability Assessment Settings

Navigation Path: Outbreak Defense > Settings > Outbreak Defense

The Vulnerability Assessment settings determine the frequency and the target of the Vulnerability Prevention scans.

Outbreak Defense > Settings ⓘ

Set up your response to vulnerabilities and outbreaks for the entire network.

Outbreak Defense **Vulnerability Assessment**

Schedule

☒ Enable Scheduled Vulnerability Prevention

☒ Daily

☐ Weekly, every Wednesday

☐ Monthly, on day 01

Start time: 02 00
hh mm

Target

☐ All groups

☒ Specified group(s)

☒ Desktops (default)

☒ Desktops 2

☒ Servers

Save

FIGURE 10-4. Vulnerability Assessment tab of Outbreak Defense Settings screen

To configure Vulnerability Assessment frequency:

1. From the **Vulnerability Assessment** tab on the **Outbreak Defense > Settings** screen, update the following options as required:
 - **Enable Scheduled Vulnerability Prevention**
 - **Frequency:** Select from **Daily**, **Weekly**, or **Monthly**. If you select **Weekly** or **Monthly**, set the day of the week or the day of the month.
 - **Start time**
 - **Target**
 - **All groups:** Scans all the clients that appear in the Group Management Tree on the **Computers** screen.
 - **Specified group(s):** Limit the vulnerability assessment scan to only the selected groups.
2. Click **Save**.

Cleanup Services

Security Agents use **Damage Cleanup Services** to protect your Windows computers against Trojan horse programs (or Trojans).

To address the threats and nuisances posed by Trojans and other malware, Cleanup does the following:

- Detects and removes live Trojans and active grayware applications
- Kills processes that Trojans and grayware applications create
- Repairs system files that Trojans and grayware modify
- Deletes files and applications that Trojans and grayware drop
- Deletes registry settings and other system changes caused by malware

To accomplish these tasks, Cleanup makes use of these components:

- **Damage cleanup engine:** the engine Cleanup uses to scan for and remove Trojans and Trojan processes
- **Damage cleanup template:** used by the Damage Cleanup Engine, this template helps identify Trojan files and processes so the Damage Cleanup Engine can eliminate them

Cleanup runs on the client on these occasions:

- You perform **Scan Now** on the client from the Web Console
- Client users run a manual **Scan**
- After hot fix or patch deployment
- When the Security Server restarts

Note: Note: Because Cleanup runs automatically, you do not need to configure it. Users are not even aware when it is executed because it runs in the background (when the client is running). However, the Security Server may sometimes notify the user to restart their computer to complete the process of removing a Trojan or grayware application.

Viewing Automatic Outbreak Defense Details

Navigation Path: Outbreak Defense > Current Status > Prevention

During an outbreak, the Security Server activates Outbreak Defense. The Automatic Outbreak Defense prevents your computers and network from being damaged by the current outbreak during the critical time when TrendLabs is creating their solution to the current outbreak.

Automatic Outbreak Defense performs the following actions during a virus outbreak:

- Blocks shared folders to help prevent viruses from infecting files in shared folders
- Blocks ports to help prevent viruses from using vulnerable ports to infect files on the network and clients.

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

- Denies write access to files and folders to help prevent viruses from modifying files
- Enables Attachment Blocking to block suspect attachment files
- Enables Content Filtering and creates a “Match All” or “Match Any” rule to filter threatening content



Chapter 11

Managing Global Settings

The topics discussed in this chapter include:

- *Configuring Global Preferences* on page 11-2
- *Internet Proxy Options* on page 11-3
- *SMTP Server Options* on page 11-5
- *Desktop/Server Options* on page 11-6
- *System Options* on page 11-13

Configuring Global Preferences

Navigation Path: Preferences > Global Settings

From the Web Console, you can configure global settings for the Security Server and for desktops and servers protected by Security Agents.

Proxy

If the network uses a proxy server to connect to the Internet, specify proxy server settings for the following services:

- Component updates and license notifications
- Web Reputation, Behavior Monitoring, and Smart Scanning

For more information, see [Internet Proxy Options](#) on page 11-3.

SMTP

The SMTP Server settings apply to all notifications and reports generated by Worry-Free Business Security.

For more information, see [SMTP Server Options](#) on page 11-5.

Desktop/Server

The Desktop/Server options pertain to the Worry-Free Business Security global settings. Settings for individual groups override these settings. If you have not configured a particular option for a group, the Desktop/Server Options are used. For example, if no URLs are approved for a particular group, all the URLs approved on this screen will be applicable for the group.

For more information, see [Desktop/Server Options](#) on page 11-6.

System

The System section of the Global Settings screen contains options to automatically remove inactive agents, check the connection of agents, and maintain the quarantine folder.

For more information, see [System Options](#) on page 11-13.

Internet Proxy Options

Navigation Path: Preferences > Global Settings > Proxy {tab}

If the network uses a proxy server to connect to the Internet, specify proxy server settings in order to utilize the following services:

- Component updates and license notifications
- Web Reputation, Behavior Monitoring, Smart Feedback, Smart Scan, and URL Filtering.

You can use the same update proxy settings or enter new credentials.

Note: The Agent will always use the same proxy server and port used by Internet Explorer to connect to the Internet for Web Reputation, Behavior Monitoring, and the Smart Protection Network. Duplicate the logon credentials you have specified for the update service only if Internet Explorer on client computers uses the same proxy server and port.

The screenshot shows the 'Proxy' tab in the Global Settings window. It is divided into two main sections:

- Settings for Updates and License Notifications:**
 - ☒ Use a proxy server for updates and license notifications
 - ☐ Use SOCKS 4/5 proxy protocol
 - Address: (For example, proxy.trend.com.tw or 123.123.123.123)
 - Port:
 - Proxy server authentication:
 - User name:
 - Password:
- Settings for Web Reputation, Behavior Monitoring, and Smart Scanning:**
 - ☒ Use the credentials specified for the update proxy (above)
 - User name:
 - Password:

FIGURE 11-1. Global Settings—Proxy Server Settings screen

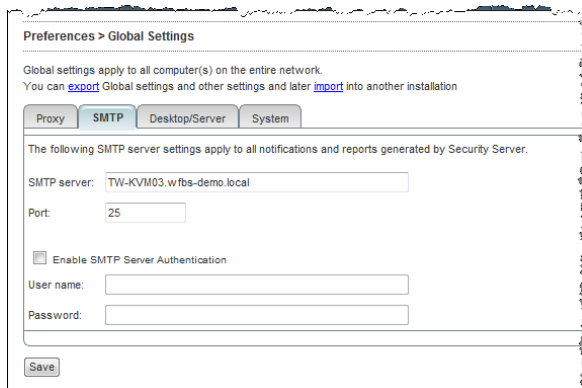
To configure Proxy Settings:

1. From the **Proxy** tab on the Global Settings screen, update the following as required:
 - **Settings for Updates and License Notifications**
 - Use a proxy server for updates and license notifications
 - Use SOCKS 4/5 proxy protocol
 - Address
 - Port
 - Proxy server authentication
 - User name
 - Password
 - **Settings for Web Reputation, Behavior Monitoring, and Smart Scanning**
 - Use the credentials specified for the update proxy
 - User name
 - Password
2. Click **Save**.

SMTP Server Options

The SMTP Server settings apply to all notifications and reports generated by WFBS.

Navigation Path: Preferences > Global Settings > SMTP {tab}



The screenshot shows the 'Preferences > Global Settings' window. At the top, there are four tabs: 'Proxy', 'SMTP' (which is selected), 'Desktop/Server', and 'System'. Below the tabs, a message states: 'Global settings apply to all computer(s) on the entire network. You can [export](#) Global settings and other settings and later [import](#) into another installation'. The main section is titled 'The following SMTP server settings apply to all notifications and reports generated by Security Server.' and contains the following fields: 'SMTP server:' with the value 'TW-KVM03.wfbs-demo.local', 'Port:' with the value '25', a checkbox for 'Enable SMTP Server Authentication' which is unchecked, 'User name:' with an empty text box, and 'Password:' with an empty text box. A 'Save' button is located at the bottom left of the form.

FIGURE 11-2. SMTP tab on the Global Settings screen

To set the SMTP server:

1. From the SMTP tab on the Global Settings screen, update the following as required:
 - **SMTP server:** The IP address or name of the SMTP server.
 - **Port**
 - **Enable SMTP Server Authentication**
 - User Name
 - Password
2. Click **Save**.

Desktop/Server Options

Navigation Path: Preferences > Global Settings > Desktop/Server {tab}

The Desktop/Server options pertain to the WFBS global settings. Settings for individual groups override these settings. If you have not configured a particular option for a group, the Desktop/Server Options are used. For example, if no URLs are approved for a particular group, all the URLs approved on this screen will be applicable for the group.

Preferences > Global Settings

Global settings apply to all computer(s) on the entire network.

Proxy SMTP **Desktop/Server** System

Location Awareness

CSM automatically identifies the location of a client based on the CSM Server Gateway information. The default setting for a VPN connection is External. To change the setting to Internal Connection, add the Gateway Address and MAC Address manually.

☒ Enable location awareness (affects Internal/External settings of [VRS](#) and [Firewall](#))

Gateway IP address: Add >>

MAC address (optional):

Gateway IP Address	Mac Address
10.1.131.254	00:13:80:28:BB:CC

General Scan Settings

☒ Exclude the Security Server database folder.

☒ Exclude Microsoft Exchange server folders when installed on Microsoft Exchange server. [?](#)

☒ Exclude Microsoft Exchange Controller folders [?](#)

Agent Uninstallation

☐ Allow the client user to uninstall Client/Server Security Agent

FIGURE 11-3. Desktop/Server tab of the Global Settings screen

To set the Desktop/Server options:

- From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:
 - [Location Awareness](#) on page 11-7
 - [Help Desk Notice](#) on page 11-7
 - [General Scan Settings](#) on page 11-8
 - [Virus Scan Settings](#) on page 11-8

- [Spyware/Grayware Scan Settings](#) on page 11-9
- [Firewall Settings](#) on page 11-9
- [URL Filtering](#) on page 11-9
- [Web Reputation](#) on page 11-10
- [IM Content Filtering](#) on page 11-10
- [Alert Settings](#) on page 11-11
- [Watchdog Settings](#) on page 11-11
- [Security Agent Uninstallation Password](#) on page 11-11
- [Security Agent Program Exit and Unlock Password](#) on page 11-12

2. Click **Save**.

Location Awareness

Location Awareness controls the In Office/Out of Office connection settings.

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Enable location awareness:** These settings will affect the In Office/Out of Office connection settings of Firewall, Web Reputation, TrendSecure, and Smart Scan.
- **Gateway Information:** Clients and connections in this list will use Internal Connection settings while remotely connecting to the network (using VPN) and Location Awareness is enabled.
 - **Gateway IP address**
 - **MAC address:** Adding the MAC address greatly improves security by permitting only the configured device to connect.

Click the corresponding trash can icon to delete an entry.

Help Desk Notice

The Help Desk Notice places a notification on the Security Agent informing the user who to contact for help. Update the following as required:

- **Label**
- **Help Desk Email Address**
- **Additional Information:** This will pop-up when the user mouses over the label

General Scan Settings

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Disable Smart Scan Service:** Switches all clients to Conventional Scan mode. Smart Scan will not be available until it is enabled again here.
- **Exclude the Security Server database folder:** Prevents Agents installed on the Security Server from scanning its own database only during Real-time Scans.

Note: By default, WFBS does not scan its own database. Trend Micro recommends preserving this selection to prevent any possible corruption of the database that may occur during scanning.

- **Exclude Microsoft Exchange server folders when installed on Microsoft Exchange server:** Prevents Agents installed on the Microsoft Exchange server from scanning Microsoft Exchange folders.
- **Exclude Microsoft Domain Controller folders:** Prevents Agents installed on the Domain Controller from scanning Domain Controller folders. These folders store user information, user names, passwords, and other important information.
- **Exclude Shadow Copy sections:** Shadow Copy or Volume Snapshot Services takes manual or automatic backup copies or snapshots of a file or folder on a specific volume.

Virus Scan Settings

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Configure scan settings for large compressed files:** Specify the maximum size of the extracted file and the number of files in the compressed file the Agent should scan.
- **Clean compressed files:** Agents will try to clean infected files within a compressed file.
- **Scan up to {} OLE layers:** Agents will scan the specified number of Object Linking and Embedding (OLE) layers. OLE allows users to create objects with one application and then link or embed them in a second application. For example, an .xls file embedded in a .doc file.

- **Add Manual Scan to the Windows shortcut menu on Clients:** Adds a **Scan with Security Agent** link to the context-sensitive menu. With this, users can right-click a file or folder (on the Desktop or in Windows Explorer) and manually scan the file or folder.

Spyware/Grayware Scan Settings

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Add cookie into spyware log:** Adds each detected spyware cookie to the spyware log.

Firewall Settings

Select the **Disable Firewall and uninstall drivers** check box to uninstall the WFBS client firewall and removes the drivers associated with the firewall.

Note: If you disable the firewall, related settings will not be available again until you re-enable the firewall.

URL Filtering

From the Desktop/Server tab of the Global Settings screen, update the following as required:

- **URLs to approve:** Separate multiple URLs with semicolons (;). Click **Add**.
- **URLs to block:** Separate multiple URLs with semicolons (;). Click **Add**.

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

Note: Use wildcards with caution as they may allow or block large sets of URLs.

The approved list takes precedence over the blocked list. When a URL matches an entry in the approved list, the URL is automatically allowed and is not checked against the blocked list.

Approved URL list: URLs in this list will not be blocked. To delete an entry, click the corresponding trash can icon.

Web Reputation

From the Desktop/Server tab of the Global Settings screen, update the following as required:

- **URLs to approve:** Separate multiple URLs with semicolons (;). Click **Add**.
- Enable SA usage logs

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

Note: Use wildcards with caution as they may allow large sets of URLs.

Approved URL list: URLs in this list will not be blocked. To delete an entry, click the corresponding trash can icon.

IM Content Filtering

Administrators can restrict the usage of certain words or phrases in instant messaging applications. Instant Messaging (IM) is a form of real-time communication between two or more people based on typed text. The text is transmitted through clients connected over a network.

Agents can restrict words used in the following IM applications:

- ICQ®
- MSN™ Messenger
- Windows Messenger Live™
- Yahoo!™ Messenger

From the **Desktop/Server** tab of the **Global Settings** screen, use the following fields as described:

- **Restricted Words:** Use this field to add restricted words or phrases. You can restrict a maximum of 31 words or phrases. Each word or phrase cannot exceed 35 characters (17 for Chinese characters). Type an entry or multiple entries separated by semicolons (;) and then click **Add>>**.

- **Restricted Words/Phrases** list: Words or phrases in this list cannot be used in IM conversations. To delete an entry, click the corresponding trash can icon.

Alert Settings

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

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

Watchdog Settings

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

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

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

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

Security Agent Uninstallation Password

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Allow the client user to uninstall Security Agent without a password.**
- **Require a password for the client user to uninstall Security Agent.**

Security Agent Program Exit and Unlock Password

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Allow the client users to exit and unlock the Security Agent on their computer without a password.**
- **Require client users to enter a password to exit and unlock the Security Agent.**

Note: Unlocking the Security Agent allows the user to override all settings configured under **Security Settings > {group} > Configure > Client Privileges**.

System Options

Navigation Path: Preferences > Global Settings > System {tab}

The System section of the Global Settings screen contains options to automatically remove inactive Agents, check the connection of Agents, and maintain the quarantine folder.

Preferences > Global Settings

Global settings apply to all computer(s) on the entire network.

Proxy SMTP Desktop/Server **System**

Remove Inactive Client/Server Security Agent

☒ Enable automatic removal of inactive Client/Server Security Agent

Automatically remove a Client/Server Security Agent if inactive for days

Connection Verification

☒ Enable scheduled verification

☐ Hourly:
☒ Daily: Start time: : (hh:mm)
☐ Weekly:

Quarantine Maintenance

Specify the capacity of the quarantine folder and the maximum file size that Client/Server Security Agent can quarantine. These settings may affect the Security Server performance during a virus outbreak.

Quarantine directory: E:\Program Files\Trend Micro\Security Server\PCCSRV\Virus

Total files quarantined: 76

Total files size: 3,483K bytes

Quarantine folder capacity: MB

Maximum size for a single file: MB

FIGURE 11-4. System tab of the Global Settings screen

To set the System options:

- From the **System** tab of the **Global Settings** screen, update the following as required:
 - Removing Inactive Security Agents* on page 11-14
 - Connection Verification* on page 11-14
 - Maintaining the Quarantine Folder* on page 11-15
- Click **Save**.

Removing Inactive Security Agents

When you use the Security Agent uninstallation program on the client to remove the Agents from a client, the program automatically notifies the Security Server. When the Security Server receives this notification, it removes the client icon from the Security Groups Tree to show that the client no longer exists.

However, if the Security Agent is removed using other methods, such as reformatting the computer's hard drive or deleting the client files manually, the Security Server will be unaware of the removal and will display the Security Agent as inactive. If a user unloads or disables the Agent for an extended time, the Security Server also displays the Security Agent as inactive.

To have the Security Groups Tree only display active clients, you can configure the Security Server to remove inactive Security Agents from the Security Groups Tree automatically.

To remove inactive Agents:

1. From the **System** tab of the **Global Settings** screen, update the following as required:
 - **Enable automatic removal of inactive Security Agent:** Enables the automatic removal of clients that have not contacted the Security Server for the specified number of days.
 - **Automatically remove a Security Agent if inactive for {} days:** The number of days that a client is allowed to be inactive before it is removed from the Web Console.
2. Click **Save**.

Connection Verification

WFBS represents the client connection status in the Security Groups Tree using icons. However, certain conditions may prevent the Security Groups Tree from displaying the correct client connection status. For example, if the network cable of a client is accidentally unplugged, the client will not be able to notify the Trend Micro Security Server that it is now offline. This client will still appear as online in the Security Groups Tree.

You can verify client-server connection manually or schedule the verification from the Web Console.

Note: Verify Connection does not allow the selection of specific groups or clients. It verifies the connection to all clients registered with the Security Server.

To verify the client-server connectivity:

1. From the **System** tab of the **Global Settings** screen, update the following as required:
 - **Enable scheduled verification:** Enables scheduled verification of Agent-Security Server communication.
 - **Hourly**
 - **Daily**
 - **Weekly, every**
 - **Start time:** The time the verification should start.
 - **Verify Now:** Instantly tests the Agents-Security Server connectivity.
2. Click **Save**.

Maintaining the Quarantine Folder

Whenever an Agent detects an Internet threat in a file and the scan action for that type of threat is quarantine, the Agent encrypts the infected file, moves it to the client's quarantine folder, and sends it to the Trend Micro Security Server quarantine folder. WFBS encrypts the infected file to prevent it from infecting other files.

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

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

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

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

Note: If the Agent is unable to send the encrypted file to the Trend Micro Security Server for any reason, such as network connection problems, the encrypted file remains in the client's quarantine folder. The Agent attempts to resend the file when it reconnects to the Trend Micro Security Server.

For more information on configuring scan settings or changing the location of the quarantine folder, see [Virus Scan Settings](#) on page 11-8.

To maintain quarantine folders:

1. From the **System** tab of the **Global Settings** screen, update the following as required:
 - **Quarantine Directory:** Change the default directory
 - **Quarantine folder capacity:** The size of the quarantine folder in MB.
 - **Maximum size for a single file:** The maximum size of a single file stored in the quarantine folder in MB.
 - **Delete All Quarantined Files:** Deletes all files in the Quarantine folder. If the folder is full and a new file is uploaded, the new file will not be stored.
2. Click **Save**.



Chapter 12

Using Logs and Reports

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

The topics discussed in this chapter include:

- [*Logs*](#) on page 12-2
 - [*Using Log Query*](#) on page 12-4
 - [*Deleting Logs*](#) on page 12-6
- [*Reports*](#) on page 12-7
 - [*One-Time Reports*](#) on page 12-8
 - [*Interpreting Reports*](#) on page 12-8
 - [*Generating Reports*](#) on page 12-11
 - [*Adding a Scheduled Report*](#) on page 12-12
 - [*Editing Scheduled Reports*](#) on page 12-13
- [*Managing Logs and Reports*](#) on page 12-14
 - [*Maintaining Reports*](#) on page 12-14
 - [*Viewing Report History*](#) on page 12-15

Logs

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

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

WFBS maintains logs under the following categories:

- Web Console event logs
- Desktop/Server logs
- Microsoft Exchange server logs (Advanced only)

TABLE 12-1. Log Type and Content

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

TABLE 12-1. Log Type and Content (Continued)

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

TABLE 12-1. Log Type and Content (Continued)

TYPE (EVENT OR ITEM THAT GENERATED THE LOG ENTRY)	CONTENT (TYPE OF LOG TO OBTAIN CONTENT FROM)
Microsoft Exchange server (Advanced only)	Virus logs Unscannable message parts logs Attachment blocking logs Content filtering logs Update logs Backup logs Archive logs Outbreak Defense logs Scan events logs Unscannable message parts logs Web Reputation logs

Using Log Query

Navigation Path: Reports > Log Query

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

Note: An MSA (Advanced only) sends its logs to the Security Server every five minutes (regardless of when the log is generated).

Reports > Log Query

Time Range

☒ Last 7 days

☐ Specified range

From: 11/28/2007 15:20
 Mid/yyyy hh mm

To: 12/5/2007 15:20
 Mid/yyyy hh mm

Type

☒ Management console events

☐ Desktop/Server

☐ Exchange server

Content

☒ Manual scan

☐ Update

☐ Outbreak Defense events

☐ Console events

Display Logs

FIGURE 12-1. Default Log Query screen

To view logs:

1. From the **Log Query** screen, update the following options as required:
 - **Time Range**
 - **Preconfigured range**
 - **Specified range:** To limit the query to certain dates.
 - **Type:** See Table 12-1 on page 12-2 to view the contents of each log type.
 - **Web Console events**
 - **Desktop/Server**
 - **Exchange Server** (Advanced only)
 - **Content:** The available options depend on the **Type** of log.
2. Click **Display Logs**.

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

Reports > Log Query > Management Console Event Logs

Results from 11/28/2007 0:00:00 to 12/5/2007 23:59:59 Records per page: 10

Export Total: 5 records Page: 1 of 1

Date/Time	Computer	Description
12/2/2007 5:00:44		Database Backup Failed
11/30/2007 15:49:57		Master Service started
11/30/2007 15:49:57		Upgrade Successful
11/30/2007 15:29:46		Master Service shut down successfully
11/28/2007 16:44:31		Master Service started

< Back

FIGURE 12-2. Sample Log Query screen

Deleting Logs

Navigation Path: Reports > Maintenance > Auto Log Deletion tab

Use the **Reports > Maintenance** screen to set up how long to keep log files and to schedule regular log maintenance.

Reports > Maintenance

Reports Auto Log Deletion Manual Log Deletion

Set up criteria for deleting older logs automatically.

Security Server

Log Type	First Log Entry	Most Recent Log Entry	Delete Log Entry Order Than
☐ Manual scan logs	03/11/2007 11:00	10/05/2007 11:00	days
☐ Update logs	03/11/2007 11:00	10/05/2007 11:00	days
☐ Outbreak Defense logs	03/11/2007 11:00	10/05/2007 11:00	days
☐ Dashboard event logs	03/11/2007 11:00	10/05/2007 11:00	days

Desktops/Servers

Log Type	First Log Entry	Most Recent Log Entry	Delete Log Entry Order Than
☐ Virus logs	03/11/2007 11:00	10/05/2007 11:00	days
	03/11/2007 11:00		days

FIGURE 12-3. Auto Log Deletion screen

To set the Security Server to delete logs that exceed a set time limit:

1. Click **Reports > Maintenance**.
2. Click the **Auto Log Deletion** tab.
3. Select the logs you want to delete.

4. In **Delete Logs Older Than**, type the number of days you want to the Security Server to retain logs.
5. Click **Save**.

Tip: To delete logs immediately, type “0” for the number of days that you want the to retain the logs.

To manually delete a log:

1. Click the **Manual Log Deletion** tab.
2. Find the row which displays the type of log to delete. Type a number in the field next to days to indicate a time limit.
3. Click **Delete**. All logs older than the amount of days you specified in step 2 are deleted.

Reports

You can manually generate One-time reports or set the Security Server to generate Scheduled reports.

You can manage the amount of reports the Security Server retains from the Maintenance screen. For One-time reports, when the number of reports exceeds the number you set, the Security Server deletes the excess reports beginning with the report that has been retained for the longest time. For Scheduled reports, set a limit of reports of each template. When the template accumulates excess reports, the Security Server deletes the excess reports beginning with the report that has been retained for the longest time.

You can print reports or send them by email to an administrator or other specified address.

To generate scheduled reports, select the contents of the report and save it as a template. To generate scheduled reports, first set up a template and then set the schedule for the template.

One-Time Reports

Navigation Path: Reports > One-time Reports

The one-time report screen contains the following items:

- **Add:** Click to open the Add Report screen.
- **Delete:** Select reports to delete and click the delete icon/link.
- **Report Name column:** Displays a list of report names. Use the checkbox to select or deselect all reports. Click the name to view the report.
- **Generated On column:** Displays the date and time the last report was generated.
- **Status column:** Displays whether the last report generated successfully.

Interpreting Reports

WFBS reports contain the following information. The information displayed could vary depending on the options selected.

TABLE 12-2. Contents of a Report

REPORT ITEM	DESCRIPTION
Antivirus	Desktop/Servers Virus Summary Virus reports show detailed information about the numbers and types of virus/malware that the scan engine detected and the actions it took against them. The report also lists the Top virus/malware names. Click the names of the virus/malware to open a new Web browser page and redirect it to the Trend Micro virus encyclopedia to learn more about that virus/malware. Top 5 Desktop/Servers with Virus Detections Displays the top five desktops or servers reporting virus/malware detections. Observing frequent virus/malware incidents on the same client might indicate that a client represents a high security risk that might require further investigation

TABLE 12-2. Contents of a Report (Continued)

REPORT ITEM	DESCRIPTION
Outbreak Defense History	Outbreak Defense History Displays recent outbreaks, the severity of the outbreaks, and identifies the virus/malware causing the outbreak and how it was delivered (by email or file).
Anti-spyware	Desktop/Servers Spyware/Grayware Summary The spyware/grayware report shows detailed information about the spyware/grayware threats detected on clients, including the number of detections and the actions that WFBS took against them. The report includes a pie chart that shows the percentage of each anti-spyware scan action that has been performed. Top 5 Desktop/Servers with Spyware/Grayware Detections The report also shows the top five spyware/grayware threats detected and the five desktops/servers with the highest number of spyware/grayware detected. To learn more about the spyware/grayware threats that have been detected, click the spyware/grayware names. A new Web browser page opens and displays related information on the spyware/grayware on the Trend Micro website.
Anti-spam summary (Advanced only)	Spam Summary Anti-spam reports show information about the number of spam and phish detected among the total amount of messages scanned. It lists the reported false positives.
Web Reputation	Top 10 Computers Violating Web Reputation Policies
URL category	Top 5 URL Category Policies Violated Lists the most commonly accessed website categories that violated the policy. Top 10 Computers Violating URL Category Policies

TABLE 12-2. Contents of a Report (Continued)

REPORT ITEM	DESCRIPTION
Behavior Monitoring	Top 5 Programs Violating Behavior Monitoring Policies Top 10 Computers Violating Behavior Monitoring Policies
Device Control	Top 10 Computer Violating Device Control Policy
Content filtering summary (Advanced only)	Content Filtering Summary Content filtering reports show information about the total number of messages that the Messaging Security Agent filtered. Top 10 Content Filtering Rules Violated A list of the top 10 content filtering rules violated. Use this feedback to fine-tune your filtering rules.
Network Virus	Top 10 Network Viruses Detected Lists the 10 network viruses most frequently detected by the common firewall driver. Click the names of the viruses to open a new Web browser page and redirect it to the Trend Micro virus encyclopedia to learn more about that virus. Top 10 Computers Attacked List the computers on your network that report the most frequent virus incidents.

Generating Reports

Navigation Path: Reports > One-time Reports or Scheduled Reports

One-time and scheduled reports are set up similarly except for setting up the schedule for scheduled reports.

Reports > One-time Reports > Add a report template

Report name:

Time Range

From: :
yyyy/M/d hh mm

To: :
yyyy/M/d hh mm

Content ☐ Select all

☒ Antivirus

☐ Outbreak Defense History

☒ Anti-spyware

☐ Anti-spam summary

☐ Web Reputation

☐ URL category

☐ Behavior Monitoring

☒ Content Filtering

☒ Network Virus

Send Report

☐ Send the report to:
For example, user1@domain.com;user2@domain.com
(Separate multiple entries with a semicolon)

☒ As a PDF attachment

☐ As a link to the report

Add

Cancel

FIGURE 12-4. Reports screen

To create or schedule a report:

1. From the **One-time Reports** screen or **Scheduled Report** screen, click **Add**.
2. Update the following options as required:
 - **Report Template:** A brief title that helps identify the report template.

- **Schedule:** Applicable only for Scheduled Reports.
 - **Daily:** The Scheduled Scan runs every day at the specified time.
 - **Weekly, every:** The Scheduled Scan runs once a week on the specified day at the specified time.
 - **Monthly, on day:** The Scheduled Scan runs once a month on the specified day at the specified time. If you select 31 days and the month has only 30 days, WFBS will not generate the report that month.
 - **Generate report at:** The time WFBS should generate the report.
 - **Time Range:** Limits the report to certain dates.
 - **Content:** To select all threats, select the **Select All** check box. To select individual threats, click the corresponding check box. Click  to expand the selection.
 - **Send the report to:** WFBS sends the generated report to the specified recipients. Separate multiple entries with semicolons (;).
 - As a PDF attachment
 - As a link to the report
3. Click **Generate/Add**.

Adding a Scheduled Report

Navigation Path: Reports > Scheduled Reports

To add scheduled reports, first set up a template and then set the schedule for the template. You can set the Security Server to deliver reports by email to an administrator or other recipient.

To set up a scheduled report template

1. From the Schedule Reports screen, click **Add**. The **Add a report template** screen appears.
2. Type a name for your report template.
3. Set the schedule that the template will use to generate individual reports. It can generate reports on a daily, weekly, and monthly basis.

4. In **Generate report at**, set the time the template will generate the individual report.

Note: Use a 24-hour clock for all time settings.

5. Under the **Content** section, select the types of threats for which you want to generate a report.
6. Select the check boxes that represent the threat types that you want to include in your report. Click to view more options.
7. Under the **Send Report** section, select the **Send the report to** checkbox and then type the email address(es) of those you want the report sent to.
8. Select how you would like the report sent:
 - As a PDF attachment
 - As a link to the report
9. Click **Add**.

Editing Scheduled Reports

Navigation Path: Reports > Scheduled Reports > {report name}

To edit a scheduled report template:

1. Modify any of the following options:
 - Enable or disable the report.
 - Report template name.
 - Set the schedule.
 - Set the **Generate report at** time.
 - Select the content.
 - Select the check box and type one or more email addresses in the **Send the report** field.
 - Select whether to send the report as a PDF file or as a link to the report.
2. Click **Save**.

Managing Logs and Reports

WFBS allows you to automate this task. Reports are based on logs, and, when the log information is deleted, reports can no longer be generated.

Maintaining Reports

Navigation Path: Reports > Maintenance > Reports tab

Specify the maximum number of reports to keep.	
Report Type	Maximum Reports to Keep (1-100)
One-time reports	10
Scheduled reports saved in each template	10
Report templates	10

Save

FIGURE 12-5. Reports Maintenance screen

Deleting reports can be a time-consuming and tedious task. Worry-Free Business Security allows you to automate this task. Reports are based on logs. When the log information is deleted, reports can no longer be generated.

From the Reports screen, you can:

Maintain Reports

To set the maximum number of reports to keep:

- From the **Reports** tab on the Maintenance screen, configure the maximum number of reports to store for the following:
 - One-time reports**
 - Scheduled reports saved in each template**
 - Report templates**
- Click **Save**.

Automatically Delete Logs

To automatically delete logs:

1. From the **Auto Log Deletion** tab on the Maintenance screen, select the **Log Type** and specify the number of days to store them.
2. Click **Save**.

Manually Delete Logs

To manually delete logs:

1. From the **Manual Log Deletion** tab on the Maintenance screen, specify the number of days to store a log type and click **Delete**.
2. Click **Save**.

Tip: To delete all the logs, specify 0 as the number of days and click **Delete**.

Viewing Report History

Navigation Path: Reports > Scheduled Reports

Scheduled Reports run according to your settings and accumulate in the Scheduled Reports screen.

To view a report history:

- From the Scheduled Reports screen, click the corresponding **Report History** link.
- To delete a Report History, select it from the list and click **Delete**.
- To send a Report History to an administrator or other person, select the **Report History** and click **Send**.



Chapter 13

Administering WFBS

This chapter explains how to use additional administrative tasks such as viewing the product license, working with the Plug-in Manager, and uninstalling the Security Server.

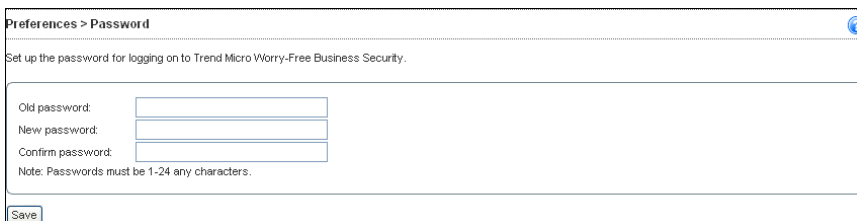
The topics discussed in this chapter include:

- *Changing the Web Console Password* on page 13-2
- *Working with the Plug-in Manager* on page 13-3
- *Viewing Product License Details* on page 13-3
- *Participating in the Smart Protection Network* on page 13-5
- *Changing the Agent's Interface Language* on page 13-6
- *Uninstalling the Trend Micro Security Server* on page 13-6

Changing the Web Console Password

Trend Micro recommends using strong passwords for the Web Console. A strong password is at least eight characters long, has one or more uppercase letters (A-Z), has one or more lowercase letters (a-z), has one or more numerals (0-9), and has one or more special characters or punctuation marks (!@#\$%^&.,:;?). Strong passwords never are the same as the user's login name or contain the login name in the password itself. They do not consist of the user's given or family name, birth dates, or any other item that is easily identified with the user.

Navigation Path: Preferences > Password



Preferences > Password

Set up the password for logging on to Trend Micro Worry-Free Business Security.

Old password:

New password:

Confirm password:

Note: Passwords must be 1-24 any characters.

Save

FIGURE 13-1. Preferences—Password screen

To change the Web Console password:

1. From the **Password** screen, update the following options as required:
 - **Old password**
 - **New password**
 - **Confirm password:** Re-type the new password to confirm.
2. Click **Save**.

Note: If you forget the Web Console password, contact Trend Micro technical support for instructions on how to gain access to the Web Console again. The only alternative is to remove and reinstall WFBS. See *Uninstalling the Trend Micro Security Server* on page 13-6.

Working with the Plug-in Manager

Navigation Path: Preferences > Plug-ins

Plug-in Manager displays the programs for both the WFBS and Agents in the Web Console as soon as they become available. You can then install and manage the programs from the Web Console, including deploying the client plug-in programs to Agents.

Download and install Plug-in Manager by clicking Plug-in Manager on the main menu of the Web Console. After the installation, you can check for available plug-in programs.

See the Plug-in’s documentation for more information.

Viewing Product License Details

Navigation Path: Preferences > Product License

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



FIGURE 13-2. Preferences–Product License screen

The Product License screen displays details about your license. Depending on the options you chose during installation, you might have a fully licensed version or an evaluation version. In either case, your license entitles you to a maintenance agreement.

When your maintenance agreement expires the clients on your network will be protected in a very limited way. Use the Product License screen to determine when your license will expire and ensure that you renew your license before it expires.

Consequences of an Expired License

When a Full-version Activation Code expires, you can no longer perform important tasks, such as downloading updated components or using Web Reputation, etc. However, unlike an evaluation-version Activation Code, when a full-version Activation Code expires, all existing configurations and other settings remain in force. This provision maintains a level of protection in case you accidentally allow your license to expire.

To renew the product license:

1. Contact your Trend Micro sales representative or corporate reseller to renew your license agreement.

Reseller Information stored in:

```
Program files\trend micro\security server\pccsrv\  
private\contact_info.ini
```

2. A Trend Micro representative will update your registration information using Trend Micro Product Registration.
3. The Security Server polls the Product Registration server and receives the new expiry date directly from the Product Registration server. You are not required to manually enter a new Activation Code when renewing your license.

Changing your License

Your Activation Code determines the type of license you have. You might have an evaluation or a fully licensed version; or you might have a Worry-Free Business Security Advanced license or a Worry-Free Business Security License. If you want to change your license, you can use the Product License screen to enter a new Activation Code.

To change your license from an evaluation version to a fully licensed version:

1. Click **Enter a new code**.
2. Type your new Activation Code in the space provided.
3. Click **Activate**.

Participating in the Smart Protection Network

Navigation Path: Preferences > Smart Protection Network

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

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

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

For more information on the Smart Protection Network, visit:

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

To enable Trend Micro Smart Feedback:

1. Click **Enable Trend Micro Smart Feedback**.
2. To send information about potential security threats in the files on your client computers, select the **Enable feedback of suspicious program files** check box.
3. To help Trend Micro understand your organization, choose the **Industry** type.
4. Click **Save**.

Changing the Agent's Interface Language

The language used on the Agent interface will correspond to the locale configured on the client operating system.

Uninstalling the Trend Micro Security Server

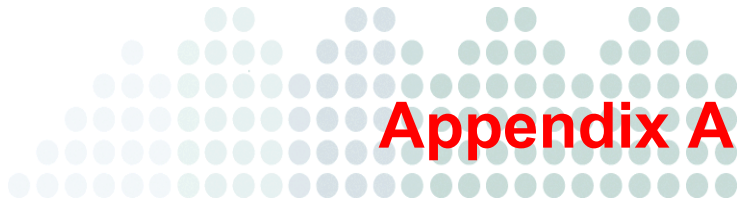
WARNING! Uninstalling Trend Micro Security Server also uninstalls the Scan Server.

WFBS uses an uninstall program to safely remove the Trend Micro Security Server from your computer. Remove the Agent from all clients before removing the Security Server.

Note: Uninstalling the Trend Micro Security Server does not uninstall Agents. Administrators must uninstall or move all Agents before uninstalling the Trend Micro Security Server. See [Removing Agents](#) on page 3-20.

To remove the Trend Micro Security Server:

1. On the computer you used to install the server, click **Start > Control Panel > Add or Remove Programs**.
2. Click **Trend Micro Security Server**, and then click **Change/Remove**. A confirmation screen appears.
3. Click **Next**. Master Uninstaller, the server uninstallation program, prompts you for the Administrator password.
4. Type the Administrator password in the text box and click **OK**. Master Uninstaller then starts removing the server files. A confirmation message appears after Security Server has been uninstalled.
5. Click **OK** to close the uninstallation program.



Client Information

This appendix explains client icons and the different types of clients.

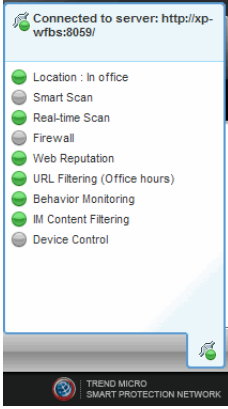
The topics discussed in this appendix include:

- *Client Icons* on page A-2
- *Location Awareness* on page A-8
- *32-bit and 64-bit Clients* on page A-8

Client Icons

Status of the WFBS Agent can be seen in three places, each displaying different information:

TABLE A-1. WFBS Agent Status locations

Tray Icon	
Client Console Flyover	 Connected to server: http://xp-wfbs:8059/ - Location : In office - Smart Scan - Real-time Scan - Firewall - Web Reputation - URL Filtering (Office hours) - Behavior Monitoring - IM Content Filtering - Device Control TREND MICRO SMART PROTECTION NETWORK
Client Console Main User Interface	 TREND MICRO Worry-Free Business Security Protection Enabled You are protected and your software is up to date Threats stopped: 0 Last scheduled scan: None Next scheduled scan: Not scheduled Virus pattern: 7,400.85 Last update: 8/22/2010 (Sun) 12:46 Next update: 8/22/2010 (Sun) 20:40 Buttons: Scan, Update Helpdesk: TREND MICRO SMART PROTECTION NETWORK

Agent Tray Icons

The following Agent Icons will display on the client machine's Windows Task Bar:

Agent Tray Icons

ICON	MEANING
	Status is normal
	(Animated) A scan is running. Could be Conventional Scan or Smart Scan. Could be Manual Scan or Scheduled Scan.
	The Agent is performing an update.
	Action is necessary: • Realtime Scan is disabled • Reboot required in order to fully clean malware • Reboot required due to an updated engine • Update is necessary Note: Open the Agent Main Console to see what action is required.

Agent FlyOver Icons

The Agent Console Flyover will open when hovering your mouse pointer over the small icon on the bottom right of the Agent Console.

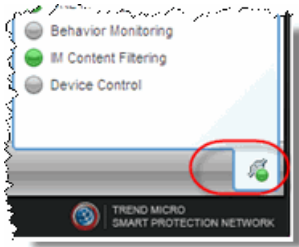


FIGURE A-1. Hover your mouse pointer to open the Agent Console Flyover.

The following table lists the Agent Console Flyover icons and their meanings:

TABLE A-2. Agent Console Flyover icons

FEATURE	ICON	MEANING
Connection	 	- Connected to Security Server - Not connect to Security Server, but real-time scan is still running. The pattern file may not be up to date. Right click on the tray icon and click Update Now.
Location	 	- In Office - Out of Office
Real Time Scan	 	- On - Off

TABLE A-2. Agent Console Flyover icons (**Continued**)

FEATURE	ICON	MEANING
Smart Scan	   	• Connected to Local Scan Server • Connected to Global Scan Server • Can't connect to the Server Smart Scan or the Trend Micro Smart Scan Server. The client is still protected under the local scan mode • Smart Scan is disabled. Using Conventional Scan Note: If clients are configured for Smart Scan but disconnected from the Smart Scan Server, verify that the Smart Scan service <code>TMiCRCSanService</code> is running and that your clients are connected to the Security Server.
• POP3 Mail Scan • Firewall • Web Reputation • URL Filtering • Behavior Monitoring • IM Content Filtering • Device Control	 	• On • Off

Agent Main Console Icons

The following image shows the Agent Console with everything up to date and working properly:



The following table lists the icons and their meanings on the Agent Console Main User Interface:

TABLE A-3. Agent Console Main User Interface icons

ICON	STATUS	WHAT YOU CAN DO
	Protection Enabled: You are protected and your software is up to date	The software is up to date and running properly. No action is required.
	Restart Computer: Restart the computer to finish fixing security threats	Security Agent has discovered threats that it cannot fix immediately. Restart the computer to finish fixing these threats.
	Protection at Risk: Contact your administrator	Real-time Scan is disabled or your protection is at risk for another reason. You must contact your administrator to resolve these security issues.
	Update Now: You have not received an update in (number) days.	The virus pattern is older than 3 days. You should update your software.
	Smart Scan Not Available: Check your Internet connection	Security Agent has not had access to the Smart Scan Server for over 15 minutes. Ensure you are connected to your network in order to scan with the latest patterns.
	Restart Computer: Restart your computer to finish installing an update	Restart your computer to finish an update.
	Updating Program: Your security software is updating	An update is in progress. Do not disconnect from the network until finished.

Location Awareness

Navigation Path: Preferences > Global Settings > Desktop/Server > Location Awareness

With Location Awareness, administrators can control security settings depending on how the client is connected to the network.

Location Awareness controls the In Office/Out of Office connection settings.

WFBS automatically identifies the location of the client based on the Worry-Free Business Security Server Gateway information and controls the websites users can access. The restrictions differ based on the user's location:

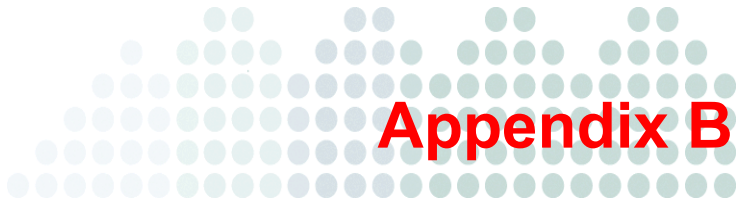
From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Enable location awareness:** These settings will affect the In Office/Out of Office connection settings of Firewall, Web Reputation, TrendSecure, and Smart Scan.

32-bit and 64-bit Clients

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

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



Using Management (Administrative and Client) Tools

This appendix explains how to use the Administrative and Client Tools that come with WFBS.

The topics discussed in this appendix include:

- *Tool Types* on page B-2
- *Administrative Tools* on page B-3
- *About the Worry-Free Remote Manager Agent* on page B-7
- *Free Disk Space* on page B-9
- *Client Tools* on page B-11
- *Add-ins* on page B-16
- *SBS and EBS Add-ins* on page B-17

Tool Types

Navigation Path: Preferences > Management Tools

WFBS includes a set of tools that can help you easily accomplish various tasks, including server configuration and client management.

Note: These tools cannot be used from the Web Console. For instructions on how to use the tools, see the relevant sections below.

These tools are classified into three categories:

- **Administrative tools:** Helps configure or manage WFBS
 - **Login Script Setup** (SetupUsr.exe): Automates the Security Agent installation.
 - **Vulnerability Scanner** (TMVS.exe): Locates unprotected computers on the network.
 - **Remote Manager Agent:** Enables Resellers to manage WFBS through a centralized Web Console.
- **Client tools:** Helps enhance the performance of the Agents.
 - **Client Packager** (ClnPack.exe): Creates a self-extracting file containing the Security Agent and components.
 - **Restore Encrypted Virus** (VSEncode.exe): Opens infected files encrypted by WFBS.
 - **Client Mover Tool** (IpXfer.exe): Transfers clients from one Security Server to another.
- **Add-ins:** These add-ins to Windows Small Business Server (SBS) 2008 and Windows Essential Business (EBS) Server 2008 allow administrators to view live security and system information from the SBS and EBS consoles. This is the same high-level information visible on the Live Status screen.

Note: Some tools available in previous versions of WFBS are not available in this version. If you require these tools, contact Trend Micro Technical Support. See [Technical Support](#) on page I-3

Administrative Tools

This section contains information about WFBS administrative tools.

Login Script Setup

With Login Script Setup, you can automate the installation of the Security Agent to unprotected computers when they log on to the network. Login Script Setup adds a program called `autopcc.exe` to the server login script. The program `autopcc.exe` performs the following functions:

- Determines the operating system of the unprotected client and installs the appropriate version of the Security Agent
- Updates the virus pattern file and program files

See [*Installing with Login Script Setup*](#) on page 3-6.

Vulnerability Scanner

Use Vulnerability Scanner to detect installed antivirus solutions and to search for unprotected computers on your network. To determine if computers are protected, Vulnerability Scanner pings ports that are normally used by antivirus solutions.

Vulnerability Scanner can perform the following functions:

- Perform a DHCP scan to monitor the network for DHCP requests so that when computers first log on to the network, Vulnerability Scan can determine their status
- Ping computers on your network to check their status and retrieve their computer names, platform versions, and descriptions
- Determine the antivirus solutions installed on the network. It can detect Trend Micro products (including OfficeScan, ServerProtect™ for Windows NT and Linux, ScanMail for Microsoft Exchange, InterScan Messaging Security Suite, and PortalProtect) and third-party antivirus solutions (including Norton AntiVirus Corporate Edition v7.5 and v7.6, and McAfee VirusScan ePolicy Orchestrator).
- Display the server name and the version of the pattern file, scan engine and program for OfficeScan and ServerProtect for Windows NT
- Send scan results through email
- Run in silent mode (command prompt mode)

- Install the Security Agent remotely on computers running Windows Server 2003 (R2)

You can also automate Vulnerability Scanner by creating scheduled tasks. For information on how to automate Vulnerability Scanner, see the TMVS Online Help.

To run Vulnerability Scanner on a computer other than the server, copy the TMVS folder from the \PCCSRV\Admin\Utility folder of the server to the computer.

Note: You cannot install the Security Agent with Vulnerability Scanner if the server component of WFBS is **present** on the same machine. Vulnerability Scanner does not install the Security Agent on a machine already **running** the server component of WFBS.

Using the Vulnerability Scanner

To configure Vulnerability Scanner:

1. In the drive where you installed the server component of WFBS, open the following directories: **Trend Micro Security Server > PCCSRV > Admin > Utility > TMVS**. Double-click **TMVS.exe**. The Trend Micro Vulnerability Scanner console appears.
2. Click **Settings**. The **Settings** screen appears.
3. In the **Product Query** box, select the products that you want to check for on your network. Select the **Check for all Trend Micro products** to select all products.
If you have Trend Micro InterScan and Norton AntiVirus Corporate Edition installed on your network, click **Settings** next to the product name to verify the port number that Vulnerability Scanner will check.
4. Under **Description Retrieval Settings**, click the retrieval method that you want to use. Normal retrieval is more accurate, but it takes longer to complete.
If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting the **Retrieve computer descriptions when available** check box.
5. To send the results to you or other Administrators automatically, under **Alert Settings**, select the **Email results to the system Administrator** check box, and then, click **Configure** to specify your email settings:

- **To**
 - **From**
 - **SMTP server:** The address of your SMTP server. For example, smtp.example.com. The SMTP server information is required.
 - **Subject**
6. To display an alert on unprotected computers, select the **Display alert on unprotected computers** check box. Then, click **Customize** to set the alert message. The **Alert Message** screen appears. You can type a new alert message or accept the default message. Click **OK**.
 7. To save the results as a comma-separated value (CSV) data file, select the **Automatically save the results to a CSV file** check box. By default, CSV data files are saved to the TMVS folder. If you want to change the default CSV folder, click **Browse**. The **Browse for folder** screen appears. Browse for a target folder on your computer or on the network and then click **OK**.
 8. You can enable Vulnerability Scanner to ping computers on the network to get their status. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout** text boxes.
 9. To remotely install the Agent and send a log to the server, type the server name and port number. To remotely install the Agent automatically, select the **Auto-install Client/Server Security Client on unprotected computer** check box.
 10. Click **Install Account** to configure the account. The **Account Information** screen appears.
 11. Type the user name and password and click **OK**.
 12. Click **OK** to save your settings. The **Trend Micro Vulnerability Scanner** console appears.

To run a manual vulnerability scan on a range of IP addresses:

1. Under **IP Range to Check**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers.

Note: The Vulnerability Scanner supports class A/B/C IP addresses.

2. Click **Start** to begin checking the computers on your network. The results are displayed in the **Results** table.

To run Vulnerability Scanner on computers requesting IP addresses from a DHCP server:

1. Click the **DHCP Scan** tab in the **Results** box. The **DHCP Start** button appears.
2. Click **DHCP Start**. Vulnerability scanner begins listening for DHCP requests and performing vulnerability checks on computers as they log on to the network.

To create scheduled tasks:

1. Under **Scheduled Tasks**, click **Add/Edit**. The **Scheduled Task** screen appears.
2. Under **Task Name**, type a name for the task you are creating.
3. Under **IP Address Range**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers.
4. Under **Task Schedule**, click a frequency for the task you are creating. You can set the task to run **Daily**, **Weekly**, or **Monthly**. If you click **Weekly**, you must select a day from the list. If you click **Monthly**, you must select a date from the list.
5. In the **Start time** lists, type or select the time when the task will run. Use the 24-hour clock format.
6. Under **Settings**, click **Use current settings** if you want to use your existing settings, or click **Modify settings**.

If you click **Modify settings**, click **Settings** to change the configuration. For information on how to configure your settings, refer to Step 3 to Step 12 in [To configure Vulnerability Scanner](#) on page B-4.

7. Click **OK** to save your settings. The task you have created appears under **Scheduled Tasks**.

Other Settings

To configure the following settings, you need to modify `TMVS.ini`:

- **EchoNum:** Set the number of clients that Vulnerability Scanner will simultaneously ping.
- **ThreadNumManual:** Set the number of clients that Vulnerability Scanner will simultaneously check for antivirus software.
- **ThreadNumSchedule:** Set the number of clients that Vulnerability Scanner will simultaneously check for antivirus software when running scheduled tasks.

To modify these settings:

1. Open the TMVS folder and locate the `TMVS.ini` file.
2. Open `TMVS.ini` using Notepad or any text editor.
3. To set the number of computers that Vulnerability Scanner will simultaneously ping, change the value for `EchoNum`. Specify a value between 1 and 64.
For example, type `EchoNum=60` if you want Vulnerability Scanner to ping 60 computers at the same time.
4. To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software, change the value for `ThreadNumManual`. Specify a value between 8 and 64.
For example, type `ThreadNumManual=60` to simultaneously check 60 computers for antivirus software.
5. To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running scheduled tasks, change the value for `ThreadNumSchedule`. Specify a value between 8 and 64.
For example, type `ThreadNumSchedule=60` to simultaneously check 60 computers for antivirus software whenever Vulnerability Scanner runs a scheduled task.
6. Save `TMVS.ini`.

About the Worry-Free Remote Manager Agent

The Trend Micro™ Worry-Free™ Remote Manager Agent allows resellers to manage WFBS with Trend Micro Worry-Free Remote Manager (WFRM). The WFRM Agent (version 2.6) is installed on the Security Servers of Worry-Free Business Security version 7.0.

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

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

Before starting the installation, ensure that you have the WFRM Agent GUID. To obtain the GUID, open the WFRM console and go to: **Customers {tab} > All Customers** (on the tree) > {customer} > **WFBS-A/7.0 > Server/Agent Details** (right pane) > **WFRM Agent Details**.

To install the Agent:

1. Go to the Security Server and navigate to the following installation folder: PCCSRV\Admin\Utility\RmAgent, and launch the application WFRMforWFBS.exe. The following is an example:
C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\WFRMforWFBS.exe.
2. Click **Yes** to signify that you are a certified partner.
3. Select **I already have a Worry-Free Remote Manager account and I want to install the Agent**.
4. Click **Next**.
5. If this is a new customer:
 - a. Select Associate with a new customer.
 - b. Click **Next**.
 - c. Enter the customer information.
 - d. Click **Next**.

Note: If the customer already exists on the WFRM Console and you use the option above “Associate with a new customer”, this will result in two customers with the same name appearing on the WFRM network tree. To avoid this, use the method below.

If this is an existing customer:

- a. Select **This product already exists in Remote Manager**.
 - b. WFBS(A) must already have been added to the WFRM console. See your WFRM documentation for instructions.
 - c. Type the GUID.
 - d. Click **Next**.
6. Select the Region and Protocol, and enter the Proxy information if required.

7. Click **Next**. The Installation Location screen opens.
8. To use the default location, click **Next**.
9. Click **Finish**.

The Agent automatically registers to the WFRM server and appears online on the WFRM console.

Free Disk Space

To maintain disk space:

- **For Desktops/Servers:**
 - Clean up quarantine files
 - Clean up log files
 - Run the Windows Disk Cleanup Utility
- **For Microsoft Exchange servers:**
 - Clean up quarantine files
 - Clean up log files
 - Run the Windows Disk Cleanup Utility
 - Clean up archive logs (for Microsoft Exchange servers only)
 - Clean up backup files (for Microsoft Exchange servers only)
 - Check size of Exchange database or transaction logs

Disk Cleaner Tool

To save disk space, the Disk Cleaner Tool (`TMDiskCleaner.exe`) identifies and deletes unused backup, log, and pattern files from the following directories:

- `{CSA}\AU_Data\AU_Temp\*`
- `{CSA}\Reserve`
- `{SS}\PCCSRV\TEMP\*` (except hidden files)
- `{SS}\PCCSRV\Web\Service\AU_Data\AU_Temp\*`
- `{SS}\PCCSRV\wss\*.log`
- `{SS}\PCCSRV\wss\AU_Data\AU_Temp\*`
- `{SS}\PCCSRV\Backup\*`

- {SS}\PCCSRV\Virus* (Deletes quarantined files older than two weeks, except the NOTVIRUS file)
- {SS}\PCCSRV\ssaptpn.xxx (keeps the latest pattern only)
- {SS}\PCCSRV\lpt\$vpn.xxx (keeps the latest three patterns only)
- {SS}\PCCSRV\icrc\$oth.xxx (keeps the latest three patterns only)
- {SS}\DBBackup* (keeps latest two subfolders only)
- {MSA}\AU_Data\AU_Temp*
- {MSA}\Debug*
- {MSA}\engine\vsapi\latest\pattern*

Use this tool either through the graphical user interface or the command line interface.

To clean unused files using the graphical user interface:

1. On the WFBS server, go to the following directory:
{SS}\PCCSRV\Admin\Utility\
2. Double-click TMDiskCleaner.exe. The Trend Micro Worry-Free Business Security Disk Cleaner appears.

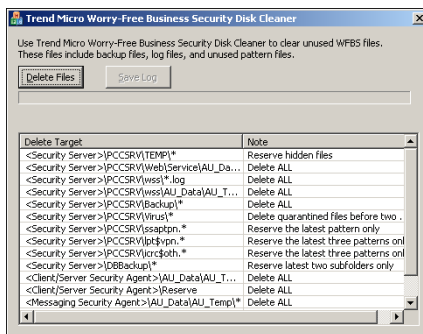


FIGURE B-1. Disk Cleaner

WARNING! Files deleted using the graphical user interface cannot be restored.

3. Click Delete Files to scan for and delete unused backup, log, and pattern files.

To clean unused files using the command line interface:

1. On the Security Server, open a Command Prompt window.
(Start --> Run --> type cmd --> click OK)
2. At the command prompt, run the following command:
`TMDiskCleaner.exe [/hide] [/log] [/allowundo]`
 - `/hide`: Runs the tool as a background process.
 - `/log`: Saves a log of the operation to `DiskClean.log` that resides in the current folder.

Note: `/log` is available only when `/hide` is used.

- `/allowundo`: Moves the files to the Recycle Bin and does not permanently delete the files.

Tip: To run the Disk Cleaner tool frequently, configure a new task using Windows Scheduled Tasks. See the Windows documentation for more information.

Client Tools

This section contains information about WFBS client tools.

Client Packager

Client Packager is a tool that can compress setup and update files into a self-extracting file to simplify delivery through email, CD-ROM, or similar media.

To run Client Packager, open the following directory:

```
..\Trend Micro Security Server\PCCSRV\Admin\Utility\  
Client Packager  
and double-click ClnPack.exe.
```

When Client Packager opens, select the OS type, the default scan method, and the output file. Then click **Create**.

Restoring an Encrypted Virus

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

Whenever a Security Agent backs up, quarantines, or renames an infected file, it encrypts the file. The quarantined file is stored in the \Suspect folder on the client, and then sent to the quarantine directory. The backup file is stored in the \Backup folder of the client, typically in C:\Program Files\Trend Micro\Client Server Security Agent\Backup\. Whenever Messaging Security Agent backs up, quarantines, or archives an email message or attachment, it encrypts the file and stores it in the MSA storage folder, typically in C:\Program Files\Trend Micro\Messaging Security Agent\storage\.

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

Note: To prevent Security Agents from detecting the virus/malware again when you use Restore Encrypted Virus, exclude the folder to which you decrypt the file from Real-time Scan.

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

Restore Encrypted Virus requires the following files:

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

Using the Graphical Interface

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

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

3. Click **Restore**.

Using the Command Line Interface

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

1. Copy VSEncrypt from the Security Server to the client:
 \PCCSRV\Admin\Utility\VSEncrypt.

WARNING! Do not copy the VSEncrypt folder to the WFBS folder. The VSAPI32.dll file of Restore Encrypted Virus will conflict with the original VSAPI32.dll.

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

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

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

Restore Encrypted Virus provides the following logs:

- VSEncrypt.log. Contains the encryption or decryption details. This file is created automatically in the temp folder for the user logged on the machine (normally, on the C: drive).

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

To encrypt or decrypt files in other locations:

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

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

Restoring Transport Neutral Encapsulation Format Email Messages

Transport Neutral Encapsulation Format (TNEF) is a message encapsulation format used by Microsoft Exchange/Outlook. Usually this format is packed as an email attachment named `Winmail.dat` and Outlook Express hides this attachment automatically. See

<http://support.microsoft.com/kb/241538/en-us>

If MSA archives this kind of email, and the extension of the file is changed to `.EML`, Outlook Express will only display the body of the email message.

Client Mover Tool

If you have more than one Security Server on the network, you can use the Client Mover tool to transfer Security Agents (SA) from one Security Server to another.

This is especially useful after adding a new WFBS server to the network when you want to transfer existing clients to the new server. Source and destination servers must be running the same version of WFBS and operating systems.

Client Mover requires the `IpXfer.exe` file.

To run Client Mover:

1. On the WFBS server, go to the following directory:
`\PCCSRV\Admin\Utility\IpXfer.`
2. Copy the `IpXfer.exe` file to the client that you want to transfer.
3. On the client, open a command prompt and then go to the folder where you copied the file.
4. Run Client Mover using the following syntax:

```
IpXfer.exe -s {server_name} -p {server_listening_port} -m 1
-c {client_listening_port}
```

where:

SYNTAX ITEM	DESCRIPTION
{server_name}	The name of the destination Security Server (the server to which the SA will transfer)
{server_listening_port}	The listening Trusted port of the destination Security Server. To view the listening port on the Security Server Web Console, click Security Settings . The port number will appear in the Security Server information bar located just above the toolbar.
1	The HTTP-based server (you must use the number "1" after "-m")
{client_listening_port}	The port number of the SA computer

To confirm that the Client now reports to the other server:

1. On the client, right click the Security Agent icon in the system tray.
2. Select **Open Worry-Free Business Security**.
3. Hover your mouse pointer over the  icon on the bottom right of the Agent interface.

- The Security Server that the SA reports to is shown at the top of the pop-up.

Note: Note: If the SA does not appear in the domain tree of the new Security Server to which it is registered, restart the new Security Server's Master Service (ofservice.exe).

Add-ins

WFBS provides add-ins to Windows™ Small Business Server (SBS) 2008 and Windows Essential Business (EBS) Server 2008. These add-ins allow administrators to view live security and system status information from the SBS and EBS consoles.

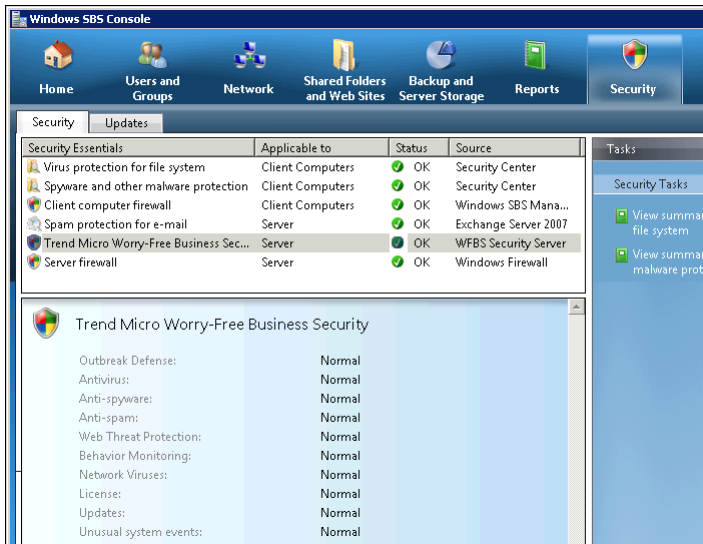


FIGURE B-2. SBS console displaying Live Status information

SBS and EBS Add-ins

Worry-Free Business Security Advanced provides add-ins to Windows Small Business Server (SBS) 2008 and Windows Essential Business (EBS) Server 2008. These add-ins allow administrators to view live security and system status information from the SBS and EBS consoles.

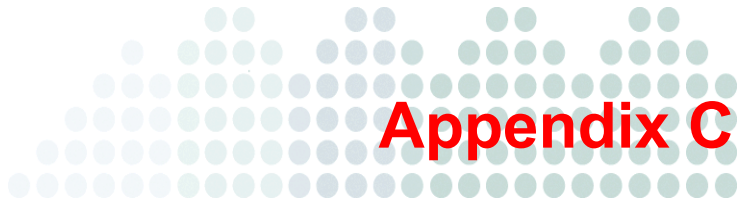
To use the SBS or EBS add-ins, open the SBS or EBS console. Under the **Security** tab, click **Trend Micro Worry-Free Business Security** to view the status information.

Installing the SBS and EBS Add-ins

The SBS or the EBS add-in installs automatically when you install the Security Server on a computer running SBS 2008 or EBS 2008. To use the add-in on another computer, you need to install it manually.

To manually install the add-in for SBS or EBS 2008:

1. Access the Web Console from the computer running SBS or EBS 2008.
2. Click **Preferences > Management Tools** and then click the **Add-ins** tab.
3. Click the corresponding **Download** link to obtain either the SBS or EBS 2008 add-in.
4. On the local computer, open the downloaded file and complete the installation.



Troubleshooting and Frequently Asked Questions

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

The topics discussed in this appendix include:

- *Troubleshooting* on page C-2
- *Frequently Asked Questions (FAQs)* on page C-11
- *Known Issues* on page C-17

Troubleshooting

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

Environments with Restricted Connections

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

If Agents can access the Security Server:

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

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

If Agents cannot access the Security Server:

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

Client Packager Post-Installation Problems

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

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

User's Spam Folder not Created (Advanced only)

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

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

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

Internal Sender-Recipient Confusion (Advanced only)

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

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

Re-sending a Quarantine Message Fails (Advanced only)

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

To resolve quarantined message failure:

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

2. Edit the entry as follows:

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

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

3. Close the Registry Editor.

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

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

- ScanMail_Master
- ScanMail_RemoteConfig

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

Saving and Restoring Program Settings

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

To restore program settings after rollback or reinstallation:

1. Stop the Trend Micro Security Server Master Service.

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

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

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

- **ofcscan.ini:** Contains global settings.
 - **ous.ini:** Contains the update source table for antivirus component deployment.
 - **Private folder:** Contains firewall and update source settings.
 - **Web\TmOPP folder:** Contains Outbreak Defense settings.
 - **Pccnt\Common\OfcPfw.dat:** Contains firewall settings.
 - **Download\OfcPfw.dat:** Contains firewall deployment settings.
 - **Log folder:** Contains system events and the verify connection log.
 - **Virus folder:** The folder in which WFBS quarantines infected files.
 - **HTTDB folder:** Contains the WFBS database.
3. Uninstall WFBS.
 4. Perform a fresh install. See the WFBS *Installation Guide*.
 5. After the master installer finishes, stop the Trend Micro Security Server Master Service on the target computer.

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

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

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

```
ComponentName=Virus pattern
```

```
Version=xxxxxxx 0 0
```

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

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

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

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

Some Components are not Installed

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

Unable to Access the Web Console

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

Browser Cache

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

SSL Certificate

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

Virtual Directory Settings

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

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

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

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

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

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

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

To enable scripts:

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

Incorrect Number of Clients on the Web Console

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

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

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

Client Icon Does Not Appear on Web Console After Installation

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

To check communication between Clients and the Web Console:

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

Issues During Migration from Other Antivirus Software

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

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

```
Uninstallation failed.
```

There are several possible causes for this error:

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

There are also several possible solutions for this error:

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

Unsuccessful Web Page or Remote Installation

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

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

Unable to Replicate Messaging Security Agent Settings (Advanced only)

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

For Windows 2003, do the first 4 steps:

1. Start **regedit**.
2. Go to
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePi
peServers\winreg`
3. Right click **winreg** > **Permissions**.
4. Add **Smex Admin Group** of target domain, and enable **Allow Read**.

Frequently Asked Questions (FAQs)

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

Where Can I Find My Activation Code and Registration Key?

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

Obtaining an Activation Code

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

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

Activation Codes have 37 characters and look like this:

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

Obtaining a Registration Key

The Registration Key can be found on:

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

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

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

Registration Keys have 22 characters and look like this:

xx-xxxx-xxxx-xxxx-xxxx

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

Registration

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

See the following website for frequently asked questions about registration:

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

Installation, Upgrade, and Compatibility

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

See the WFBS *Installation Guide* for information.

Which Agent installation method is best for my network environment?

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

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

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

Does WFBS support 64-bit platforms?

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

Can I upgrade to WFBS from Trend Micro™ ServerProtect?

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

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

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

How Can I Recover a Lost or Forgotten Password?

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

Intuit Software Protection

What happens when an attempted Intuit update is blocked?

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

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

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

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

Configuring Settings

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

You can download all WFBS documentation from the following site:

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

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

See the following tables for the SBS 2003 exclusions:

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

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

TABLE C-2. IIS Exclusions

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

TABLE C-3. Domain Controller Exclusions

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

TABLE C-4. Windows SharePoint Services Exclusions

Temporary SharePoint folder	C:\windows\temp\FrontPageTempDir

TABLE C-5. Client Desktop Folder Exclusions

Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore

TABLE C-6. Additional Exclusions

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

Do I Have the Latest Pattern File or Service Pack?

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

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

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

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

- The Trend Micro Update Center:
<http://www.trendmicro.com/download/>
- The Trend Micro Pattern File:
<http://www.trendmicro.com/download/pattern.asp>

Smart Scan

What is Smart Scan?

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

Is Smart Scan reliable?

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

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

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

TMiCRCSanService

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

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

Known Issues

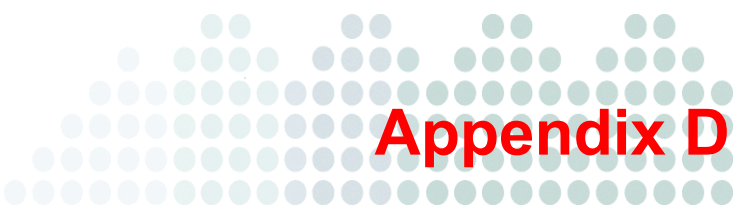
Known issues are features in WFBS software that may temporarily require a workaround. Known issues are typically documented in the Readme document you received with your product. Readme files for Trend Micro products can also be found in the Trend Micro Update Center:

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

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

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

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



Appendix D

Trend Micro Services

This appendix explains the services that Trend Micro offers.

The topics discussed in this appendix include:

- *Outbreak Prevention Policy* on page D-2
- *Damage Cleanup Services* on page D-2
- *Vulnerability Assessment* on page D-3
- *IntelliScan* on page D-4
- *ActiveAction* on page D-4
- *IntelliTrap* on page D-6
- *Email Reputation Services (Advanced only)* on page D-7
- *Web Reputation* on page D-8

Outbreak Prevention Policy

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

The Outbreak Prevention Policy is downloaded from Trend Micro to the Trend Micro Security Server.

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

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

- Blocks shared folders to help prevent virus/malware from infecting files in shared folders
- Blocks ports to help prevent virus/malware from using vulnerable ports to infect files on the network and clients
- Denies write access to files and folders to help prevent virus/malware from modifying files

Damage Cleanup Services

WFBS uses Damage Cleanup Services (DCS) to protect your Windows computers against Trojans (or Trojan horse programs) and virus/malware.

The Damage Cleanup Services Solution

To address the threats posed by virus/malware or spyware/grayware, DCS does the following:

- Detects and removes threats
- Kills processes that threats create
- Repairs system files that threats modify
- Deletes files and applications that threats create

To accomplish these tasks, DCS makes use of these components:

- **Damage Cleanup Engine:** The engine Damage Cleanup Services uses to scan for and remove threats and its associated processes.
- **Damage Cleanup Template:** Used by the Damage Cleanup Engine, this template helps identify threats and its associated processes so the engine can eliminate them.

In WFBS, DCS runs on the client on these occasions:

- Users run Manual or Scheduled Scan.
- After hot fix or patch deployment.
- When the WFBS service is restarted.

Because DCS runs automatically, you do not need to configure it. Users are not even aware when it is executed because it runs in the background (when the Agent is running). However, WFBS may sometimes notify the user to restart their client to complete the process of removing threats.

Vulnerability Assessment

Vulnerability Assessment provides system Administrators the ability to assess security risks to their networks. The information they generate by using Vulnerability Assessment gives them a clear guide as to how to resolve known vulnerabilities and secure their networks.

Use Vulnerability Assessment to:

- Configure tasks that scan any or all computers attached to a network. Scans can search for single vulnerabilities or a list of all known vulnerabilities.
- Run manual assessment tasks or set tasks to run according to a schedule.
- Create reports that identify vulnerabilities according to individual computers and describe the security risks those computers present to the overall network. The reports identify the vulnerability according to standard naming conventions so that Administrators can research further to resolve the vulnerabilities and secure the network.
- View assessment histories and compare reports to better understand the vulnerabilities and the changing risk factors to network security.

IntelliScan

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

Using IntelliScan provides the following benefits:

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

ActiveAction

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

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

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

Using ActiveAction provides the following benefits:

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

Default ActiveAction Settings

The default ActiveAction settings for the following threats are:

TABLE D-1. Default ActiveAction Settings

THREAT	ACTION	ACTION FOR UNCLEANABLE THREATS
Virus	Clean	2nd action: delete if backup is on: backup copy is quarantined (backup is only default)
Spyware/ Grayware	Quarantine	-
Worm/Trojans	Quarantine	-
Packer	Quarantine	-
Probable malware	Pass	-
Cookie	Delete	-
Other malware	Clean	2nd action: delete if backup is on: backup copy is quarantined (backup is only default)

Note: Future pattern files could update the default actions.

IntelliTrap

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

Note: IntelliTrap uses the same scan engine as virus scanning. As a result, the file handling and scanning rules for IntelliTrap will be the same as the ones the administrator defines for virus scanning.

Agents write bot and other malware detections to the IntelliTrap log. You can export the contents of the IntelliTrap log for inclusion in reports.

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

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

True File Type

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

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

For example, .gif files make up a large volume of all Web traffic, but they are unlikely to harbor virus/malware, launch executable code, or carry out any known or theoretical exploits. Therefore, does this mean they are safe? Not entirely. It is possible for a

malicious hacker to give a harmful file a “safe” file name to smuggle it past the scan engine and onto the network. This file could cause damage if someone renamed it and ran it.

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

Email Reputation Services (Advanced only)

Email Reputation technology determines spam based on the reputation of the originating Mail Transport Agent (MTA). This off-loads the task from the WFBS server. With Email Reputation enabled, all inbound SMTP traffic is checked by the IP databases to see whether the originating IP address is clean or it has been black-listed as a known spam vector.

There are two service levels for Email Reputation:

- **Standard:** The Standard service uses a database that tracks the reputation of about two billion IP addresses. IP addresses that have been consistently associated with the delivery of spam messages are added to the database and rarely removed.
- **Advanced:** The Advanced service level is a DNS, query-based service like the Standard service. At the core of this service is the standard reputation database, along with the dynamic reputation, real-time database that blocks messages from known and suspected sources of spam.

When an email message from a blocked or a suspected IP address is found, Email Reputation Services (ERS) stops it before it reaches your messaging infrastructure. If ERS blocks email messages from an IP address you feel is safe, add that IP address to the Approved IP Address list.

Web Reputation

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

If Web Reputation blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list. For information on adding a URL to the Approved URL list, see [Configuring Global Settings](#).

Reputation Score

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

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

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



Trend Micro Security *for Mac* Plug-in

Topics in this appendix:

- *About Trend Micro Security for Mac* on page E-2
- *The Trend Micro Security Client* on page E-3
- *Installing the Trend Micro Security Server for MAC* on page E-4
- *Installing the Trend Micro Security Client* on page E-21
- *Keeping Protection Up-to-Date* on page E-32
- *Protecting Computers from Security Risks* on page E-38
- *Managing the Trend Micro Security Server and Clients* on page E-60
- *Troubleshooting and Support* on page E-69

About Trend Micro Security *for Mac*

Trend Micro™ Security *for Mac* provides the latest endpoint protection against security risks, blended threats, and platform independent web-based attacks. Trend Micro Security *for Mac* integrates with Trend Micro™ Worry-Free™ Business Security, simplifying the management of Macintosh desktops, laptops, and servers through the same Web Console that manages Windows-based clients and servers.

Note: Many features of the Trend Micro Security for Mac plug-in are similar but not always identical to the features of the main application, Worry-Free Business Security. Do not confuse these.

The Trend Micro Security Server

The Trend Micro Security Server is the central repository for all client configurations, security risk logs, and updates.

The server performs two important functions:

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

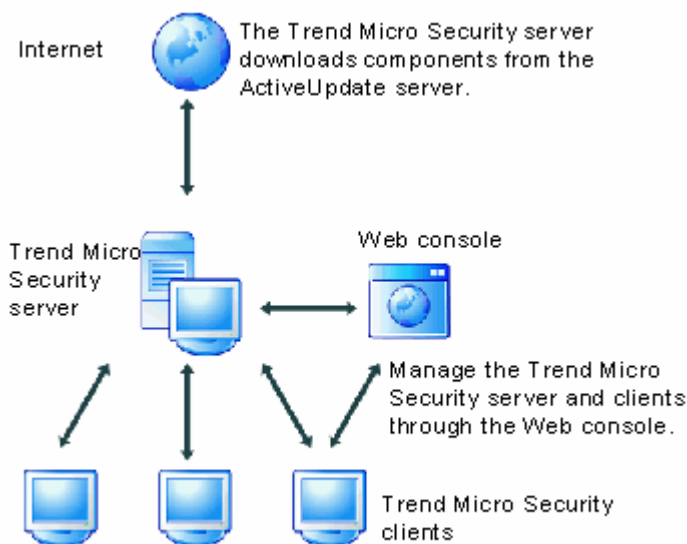


FIGURE E-1. How the Trend Micro Security Server works

Trend Micro Security provides real-time, bidirectional communication between the server and clients. Manage the clients from a browser-based Web Console which you can access from virtually anywhere on the network. The server communicates with the client through the ActiveMQ™ protocol.

The Trend Micro Security Client

Protect Macintosh computers from security risks by installing the Trend Micro Security client on each computer. The client provides three scan types: *Real-Time Scan* on page E-42, *Scheduled Scan* on page E-44, and *Manual Scan* on page E-43.

The client reports to the parent server from which it was installed. The client sends events and status information to the server in real time. Clients communicate with the server through the ActiveMQ protocol.

Installing the Trend Micro Security Server for MAC

Server Installation Requirements

This section details software, hardware, and operating system requirements for installing Trend Micro Security for Mac server.

To install Trend Micro Security for Mac server, you must first have the following software products:

- Trend Micro™ Worry-Free™ Business Security server, version 7
- Plug-in Manager, version 1.5 with the latest patch

Note: Refer to the Plug-in Manager readme for instructions on installing Plug-in Manager.

- Microsoft™ .NET Framework 2.0

The following third-party programs will be installed automatically:

- Microsoft SQL Server 2005 Express
- Apache™ ActiveMQ 5.2.0
- Microsoft Data Access Components (MDAC) 2.81 on Windows 2000 computers
- Microsoft Visual C++ 2005 Redistributable

Operating System Requirements

The following are the operating system requirements for installing the Trend Micro Security Server:

TABLE E-1. Trend Micro Security for Macintosh Server operating system requirements

SERIES OR FAMILY	SUPPORTED SERVICE PACKS OR RELEASES
Windows 7	For each of the following, no service pack or with service pack (SP) 1 (public beta) • Ultimate Edition • Enterprise Edition • Professional Edition • Home Premium Edition • Home Basic Edition
Windows Vista	For each of the following, with SP1 or SP2: • Ultimate edition • Enterprise Edition • Business Edition • Home Premium Edition • Home Basic Edition
Windows XP	For each of the following, with SP2 or SP3: • Home edition • Professional edition • Media Center 2005 edition • Tablet PC 2005 edition
Windows Server 2008	For each of the following, no service pack or SP2: • Standard Edition • Enterprise Edition • Datacenter Edition
Windows Server 2008 R2	• Standard • Enterprise

TABLE E-1. Trend Micro Security for Macintosh Server operating system requirements (Continued)

SERIES OR FAMILY	SUPPORTED SERVICE PACKS OR RELEASES
Windows Storage Server 2008	• no service pack
Windows Small Business Server 2008	• Standard Edition, no service pack or SP2 • Premium Edition, no service pack or SP2
Windows SBS 2008 R2	• SP1
Windows Essential Business Server (EBS) 2008	• no service pack
Windows Server 2008 Foundation	• no service pack and SP2
Windows Home Server V2 (code name: Vail and Aurora)	• no service pack (public beta)
Windows Server 2003	• Web Edition with SP2 • Standard Edition with SP2 • Enterprise Edition with SP2 • Datacenter Edition with SP2
Windows Server 2003 R2	• Standard Edition with SP2 • Enterprise Edition with SP2 • Datacenter Edition with SP2
Windows SBS 2003	• SP2

TABLE E-1. Trend Micro Security for Macintosh Server operating system requirements (Continued)

SERIES OR FAMILY	SUPPORTED SERVICE PACKS OR RELEASES
Windows SBS 2003 R2	• no service pack
Windows Storage Server 2003	• SP2
Windows Storage Server 2003 R2	• SP2
Windows Home Server	• no service pack or SP1

Hardware Requirements

See [Table E-2](#) for the hardware requirements for installing this plug-in.

Note: Both the Worry-Free Business Security Server and the Plug-In Manager must already be installed before you can install the Trend Micro Security (for Mac) server. The system requirements in [Table E-2](#) below are for the Trend Micro Security Server only.

TABLE E-2. Trend Micro Security for Mac hardware requirements

RESOURCE	REQUIREMENT
RAM	512MB minimum, 1GB recommended
Available disk space	With Worry-Free™ Business Security Server installed on the system drive (usually, C: drive): • 1.5GB minimum Note: Trend Micro Security Server always installs on the same drive as the Worry-Free server. With Worry-Free server installed on a drive other than the system drive: • 600MB minimum on the drive where the Worry-Free server is installed. • 900MB minimum on the system drive. Third-party programs used by Trend Micro Security Server (such as Microsoft SQL Server 2005 Express™) will be installed on this drive.

Update Source

To change the Plug-in Manager update source, modify the following setting in the {SS}\PCCSRV\Private\ofcserver.ini file:

```
[INI_UPDATE_SETTING]
```

```
PLMUpdateSource={update server}
```

for example, change {update server} to:

```
http://wfbs.activeupdate.example.com/activeupdate/wfbs7
```

Server Installation

Install the Trend Micro Security Server by performing the following steps:

Note: To upgrade the server, see *Upgrading the Server and Clients* on page E-60.

To install Trend Micro Security Server:

1. Open the Worry-Free Business Security Web Console and click **Preferences > Plug-Ins** on the main menu.

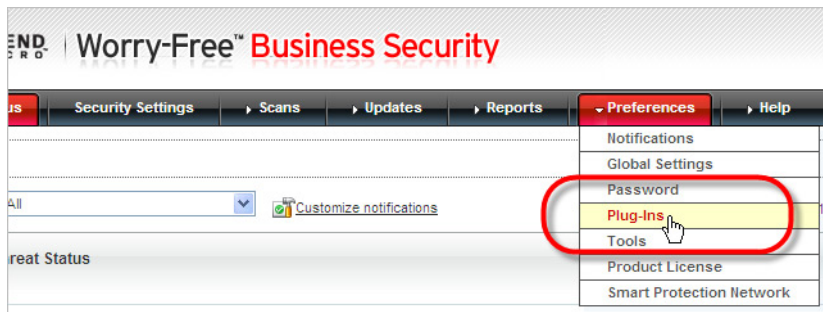


FIGURE E-2. Worry-Free Business Security Web Console Preferences menu showing Plug-Ins menu item

2. Go to the **Trend Micro Security (for Mac)** section and click **Download**.

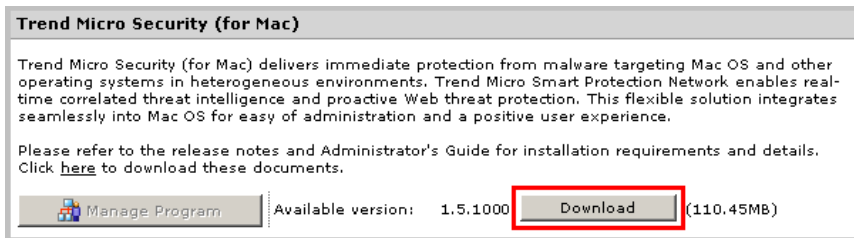


FIGURE E-3. Trend Micro Security download button

Note: Plug-in Manager downloads the package to
{WFBS server installation folder}\
PCCSRV\Download\Product.

{WFBS server installation folder} is typically
C:\Program Files\Trend Micro\Security Server.

3. Monitor the download progress. You can navigate away from the screen during the download.



FIGURE E-4. Trend Micro Security (for Mac) Download progress

If you encounter problems downloading the package, check the server update logs on the Worry-Free Business Security Web Console. On the main menu, click **Reports > Log Query**.

4. After Plug-in Manager downloads the package, a new screen with the following options displays: **Install Now** or **Install Later**.

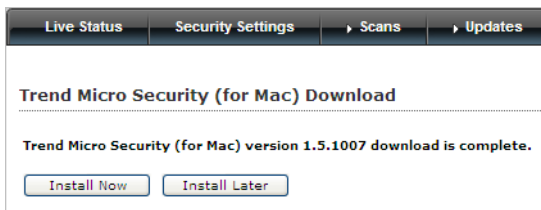


FIGURE E-5. Download complete

5. If you click **Install Now**, agree to the license agreement (shown in [Figure E-6](#)) and then check the installation progress.

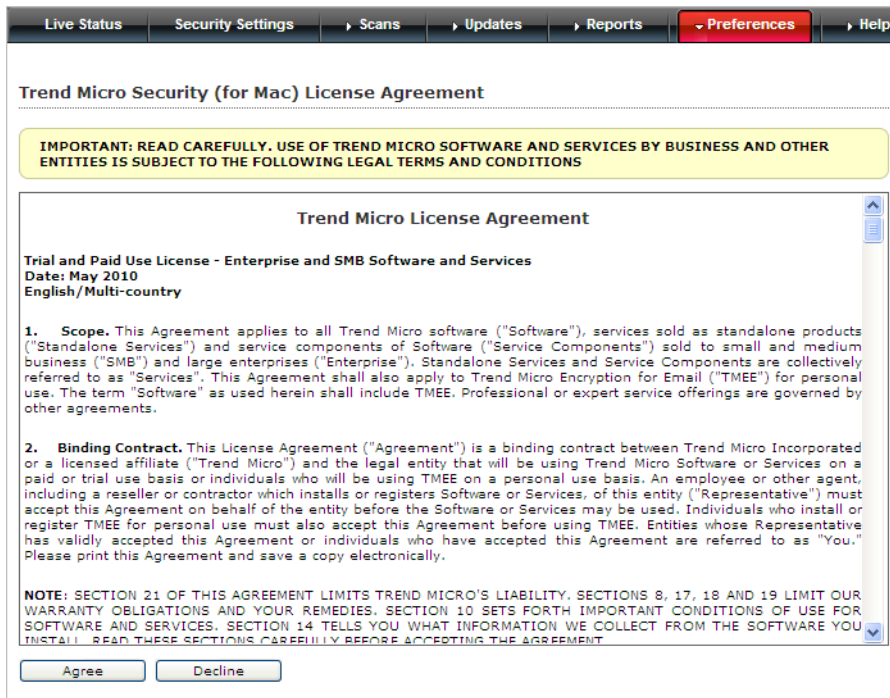


FIGURE E-6. Trend Micro Security (for Mac) License Agreement screen

6. If you click **Install Later**:
 - a. Open the Worry-Free Business Security Web Console and click **Preferences > Plug-Ins** on the main menu.
 - b. Go to the **Trend Micro Security (for Mac)** section and click **Install**.
 - c. Agree to the license agreement and then check the installation progress.

After the installation, the Trend Micro Security version displays.

Server Post-Installation

Perform the following tasks immediately after installing the Trend Micro Security Server:

1. Verify the following:
 - The following services display on the Microsoft Management Console:
 - ActiveMQ for Trend Micro Security
 - SQL Server (TMSM)
 - Trend Micro Security for (Mac)
 - When you open Windows Task Manager, the TMSMainService.exe process is running.
 - The following registry key exists:
HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_TMSM
 - The Trend Micro Security Server files are found under the {Server installation folder}.
2. Open the Worry-Free Business Security Web Console and click **Preferences > Plug-Ins** on the main menu.
3. Go to the **Trend Micro Security for (Mac)** section and click **Manage Program**.

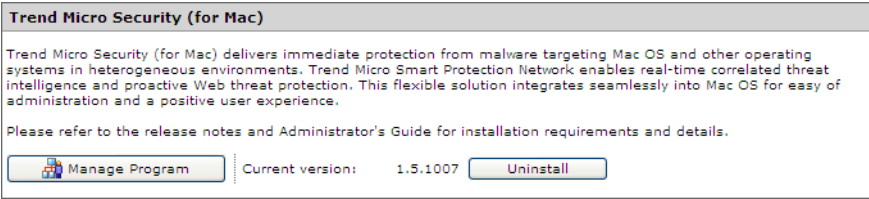


FIGURE E-7. Manage Program button

4. Type the Activation Code for the product and click **Save**. The Activation Code is case-sensitive.

Trend Micro Security (for Mac)

Start to use Trend Micro Security (for Mac).
Type your Activation Code below to activate Trend Micro Security for Mac or click [Trial Version](#) to begin your trial.

Activation Code

Product: Trend Micro Security (for Mac)

Activation Code: - - - - - -

[Save](#)

FIGURE E-8. Activation Code screen

If you do not have the Activation Code, you can click **Trial Version** to start a 30-day evaluation or register online at the Trend Micro registration website. After you complete the registration, Trend Micro sends an email with the Activation Code. You can then continue with activation.

If you have activated an evaluation version license, ensure that you upgrade to the full version before the license expires.

If the Activation Code is correct, a screen with the license details displays.

Trend Micro Security (for Mac)

License

Status: Activated

Version: Evaluation - [View license upgrade instructions](#)

Seats: 200

License expires on: Friday, December 31, 2010

Activation Code: [blurred]

[Launch](#)

FIGURE E-9. License details screen

5. Click **Launch** to open the Web Console.

Server Uninstallation

You can uninstall Trend Micro Security Server from the Plug-in Manager screen on the Web Console.

To uninstall the Trend Micro Security Server:

1. Open the Worry-Free Business Security Web Console and click **Plug-in Manager** on the main menu.
2. Go to the **Trend Micro Security for (Mac)** section and click **Uninstall**.
3. Monitor the uninstallation progress. You can navigate away from the screen during the uninstallation. After the uninstallation is complete, the Trend Micro Security Server is again available for installation.

Note: The uninstallation package does not remove Java runtime environment (JRE) 1.6 Update 14. You can remove JRE if no other application is using it.

Getting Started with Trend Micro Security

The Web Console

The Web Console is the central point for monitoring Trend Micro Security clients and configuring settings to be deployed to clients. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications.

Use the Web Console to do the following:

- Manage clients installed on Macintosh computers
- Organize clients into logical groups for simultaneous configuration and management
- Set scan configurations and initiate scanning on a single or multiple computers
- Configure security risk notifications and view logs sent by clients
- Configure outbreak criteria and notifications

Open the Web Console from any computer on the network that has the following resources:

- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft™ Internet Explorer™ 6.0 or later

To open the Web Console:

1. On a web browser, type the Worry-Free Business Security Server URL.
2. Type the user name and password to log on to the Worry-Free Business Security Server.
3. On the main menu, click **Preferences > Plug-Ins**.
4. Go to the **Trend Micro Security for (Mac)** section and click **Manage Program**.

Security Summary

The Summary screen appears when you open the Trend Micro Security Web Console or click **Summary** in the main menu.

Tip: Refresh the screen periodically to get the latest information.

Networked Computers

The **Networked Computers** section displays the following information:

- The connection status of all Trend Micro Security clients with the Trend Micro Security Server. Clicking a link opens the client tree where you can configure settings for the clients.
- The number of detected security risks and web threats
- The number of computers with detected security risks and web threats. Clicking a number opens the client tree displaying a list of computers with security risks or web threats. In the client tree, perform the following tasks:
 - Select one or several clients, click **Logs > Security Risk Logs**, and then specify the log criteria. In the screen that displays, check the **Results** column to see if the scan actions on the security risks were successfully carried out. For a list of scan results, see [Scan Results](#) on page E-55.

- Select one or several clients, click **Logs > Web Reputation Logs**, and then specify the log criteria. In the screen that displays, check the list of blocked websites. You can add websites that you do not want blocked to the list of approved URLs. See *Approved URLs* on page E-58.

Components and Program

The **Update Status for Networked Computers** table contains information about Trend Micro Security components and the client program that protects Macintosh computers from security risks.

Update outdated components immediately. You can also upgrade clients to the latest program version or build if you recently upgraded the server. For client upgrade instructions, see *Upgrading the Server and Clients* on page E-60.

To launch an update from the Summary screen:

1. Go to the **Update Status for Networked Computers** section and click the link under the **Outdated** column. The client tree opens, showing all the clients that require an update.
2. Select the clients to update.
3. Click **Tasks > Update**. Clients that receive the notification start to update. On Macintosh computers, the Trend Micro Security icon on the menu bar indicates that the product is updating. Users cannot run any task from the console until the update is complete.

The Trend Micro Security Client Tree

The client tree, in the Client Management tab, displays all the clients that the server currently manages. All clients belong to a certain group. Use the menu items above the client tree to simultaneously configure, manage, and apply the same configuration to all clients belonging to a group.

Client Tree General Tasks

Below are the general tasks that you can perform when the client tree displays:

- Click the root icon  to select all groups and clients. When you select the root icon and then choose a menu item above the client tree, a screen for configuring settings displays. On the screen, after selecting or typing your configuration choices, click one of the following general options:
 - **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing or future group. Future groups are groups not yet created at the time you configure the settings.
 - **Apply to Future Groups Only:** Applies settings only to clients added to future groups. This action does not apply settings to new clients added to an existing group.
- To select multiple adjacent groups or clients, click the first group or client in the range, hold down the SHIFT key, and then click the last group or client in the range.
- To select a range of non-contiguous groups or clients, hold down the CTRL key and then click the groups or clients that to select.
- Search for a client to manage by specifying a full or partial client name in the **Search for computers** text box. A list of matching client names will appear in the client tree.
- Sort clients based on column information by clicking the column name.

Client Tree Specific Tasks

Above client tree are menu items that allow you perform the following tasks:

TABLE E-3. Client tree specific tasks

MENU BUTTON	TASK
Tasks	• Update client components. See <i>Client Update</i> on page E-37. • Run Scan Now on client computers. See <i>Scan Now</i> on page E-45.
Settings	• Configure scan settings. See the following topics: • <i>Manual Scan</i> on page E-43 • <i>Real-Time Scan</i> on page E-42 • <i>Scheduled Scan</i> on page E-44 • <i>Scan Exclusions</i> on page E-48 • Configure web reputation policies. See <i>Web Reputation Policies</i> on page E-57.
Logs	View the following log types: • <i>Security Risk Logs</i> on page E-54 • <i>Web Reputation Logs</i> on page E-59
Manage Client Tree	Manage Trend Micro Security groups: • Add Group • Rename Group • Move Client • Remove Group/Client See <i>Trend Micro Security Groups</i> on page E-20.

Trend Micro Security Groups

A group in Trend Micro Security is a set of clients that share the same configuration and run the same tasks. By organizing clients into groups, you can simultaneously configure, manage, and apply the same configuration to all clients belonging to the groups.

For ease of management, group clients based on their departments or the functions they perform. You can also group clients that are at a greater risk of infection to apply a more secure configuration to all of them.

You can add or rename groups, move clients to a different group, or remove clients permanently. A client removed from the client tree is not automatically uninstalled from the client computer. The Trend Micro Security client can still perform server-dependent tasks, such as updating components. However, the server is unaware of the existence of the client and therefore cannot send configurations or notifications to the client.

If the client has been uninstalled from the computer, it is not automatically removed from the client tree and its connection status is "Offline". Manually remove the client from the client tree.

To add a group:

1. Go to **Client Management > Manage Client Tree > Add Group**
2. Type a name for the group you want to add.
3. Click **Add**. The new group appears in the client tree.

To rename a group:

1. Go to **Client Management > Manage Client Tree > Rename Group**
2. Type a new name for the group.
3. Click **Rename**. The new group name appears in the client tree.

To move a client:

1. Go to **Client Management > Manage Client Tree > Move Client**
2. Select the group to which to move the client.
3. Decide whether to apply the settings of the new group to the client.

Tip: Alternatively, drag and drop the client to another group in the client tree.

4. Click **Move**.

To delete a group or client:

1. Go to **Client Management > Manage Client Tree > Remove Group/Client**
2. Before deleting a group, check if there are clients that belong to the group and then move them to another group. The procedure for moving clients is found below.
3. When the group is empty, select the group and click **Remove Group/Client**.
4. To delete a client, select the client and click **Remove Group/Client**.

Installing the Trend Micro Security Client

Client Installation Requirements

The following are the requirements for installing the Trend Micro Security client on a Macintosh computer.

TABLE E-4. Client installation requirements

RESOURCE	REQUIREMENT
Operating system	Desktop and Server versions: • Mac OS™ X Snow Leopard™ 10.6 or later • Mac OS X version 10.5.6 (Leopard™) or later • Mac OS X version 10.4.11 (Tiger™) or later
Hardware	• Processor: PowerPC™ or Intel™ core processor • RAM: 256MB minimum • Available disk space: 30MB minimum
Others	• Java for Mac OS X 10.4, Release 9 • Java for Mac OS X 10.5, Update 4

Client Installation Methods

There are two ways to install the Trend Micro Security client.

- Install on a single computer by launching the installation package on the Macintosh computer
- Install on several computers by using Apple Remote Desktop

Note: To upgrade clients, see [Upgrading the Server and Clients](#) on page E-60.

Obtain the client installation package (tmsminstall.mpkg.zip) from the Trend Micro Security Server and copy it to the Macintosh computer. To obtain the package, perform any of the following steps:

- On the Trend Micro Security Server Web Console, navigate to **Administration > Client Setup Files** and click the link under **Client Installation File**.

Note: The link to the client uninstallation file is also available on this screen. Use this program to remove the client program from the Macintosh computer. For information on uninstalling the Trend Micro Security client, see [Client Uninstallation](#) on page E-31.

- Navigate to {Server installation folder}\
TMSM_HTML\ClientInstall and search for the file tmsminstall.mpkg.zip.

Installing on a Single Computer

The process of installing Trend Micro Security client on a single computer is similar to the installation process for other Macintosh software.

During the installation, users may be prompted to allow connections to **icorepluginMgr**, which is used to register the client to the server. Instruct users to allow the connection when prompted.

To install on a single Macintosh computer:

1. Check for and uninstall any security software on the Macintosh computer.
2. Obtain the client installation package tmsminstall.mpkg.zip. For information on obtaining the package, see [Client Installation Methods](#) on page E-22.

3. Copy and then launch the package on the Macintosh computer. Launching the package unarchives the file `tmsminstall.mpkg`.

WARNING! The files on the package may become corrupted if users launch the package using archiving tools not built-in on the Mac. Instruct users to launch the package using built-in archiving tools, such as Archive Utility.

To launch the file from the command line, use the following command:

```
ditto -xk tmsminstall.mpkg.zip  
{destination folder}
```

4. Launch `tmsminstall.mpkg`. When a message prompting you to continue with installation displays, click **Continue**.

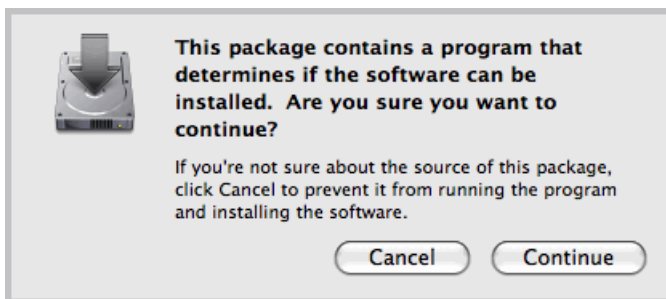


FIGURE E-10. Confirm installation message

5. On the Introduction screen, click **Continue** to proceed.



FIGURE E-11. Introduction screen

6. On the Installation Type screen, click **Install**.



FIGURE E-12. Installation Type screen

7. Fill in the **Name** and **Password** fields to begin the installation process.

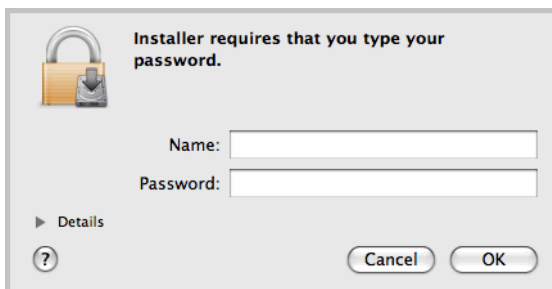


FIGURE E-13. Message prompting for user name and password

Note: Specify the name and password for an account with administrative rights on the Macintosh computer.

8. If the installation was successful, click **Close** to finish the installation process. The client automatically registers to the server where the client installation package was obtained. The client also updates for the first time.

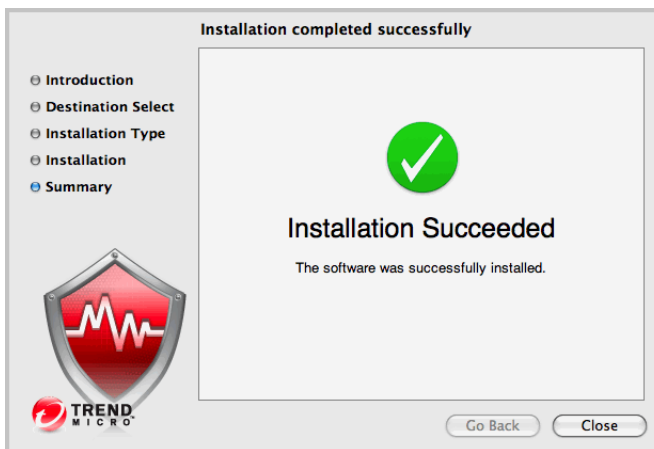


FIGURE E-14. Installation Succeeded screen

9. Perform client postinstallation tasks (See *Client Postinstallation* on page E-29).

Installing on Several Computers

The process of installing Trend Micro Security client on several computers can be simplified by using Apple Remote Desktop.

To install on several Macintosh computers:

1. Check for and uninstall any security software on the Macintosh computers.
2. Obtain the client installation package `tmsminstall.mpkg.zip`. For information on obtaining the package, see [Client Installation Methods](#) on page E-22.
3. Copy and then launch the package on the Macintosh computer with Apple Remote Desktop. Launching the package unarchives the file `tmsminstall.mpkg`.

WARNING! The files on the package may become corrupted if users launch the package using archiving tools not built-in on the Mac. Instruct users to launch the package using built-in archiving tools, such as Archive Utility.

To launch the file from the command line, use the following command:

```
ditto -xk tmsminstall.mpkg.zip  
{destination folder}
```

4. Open Apple Remote Desktop on the Macintosh computer.
5. Select the computers to which to install the Trend Micro Security client and then click **Install**.

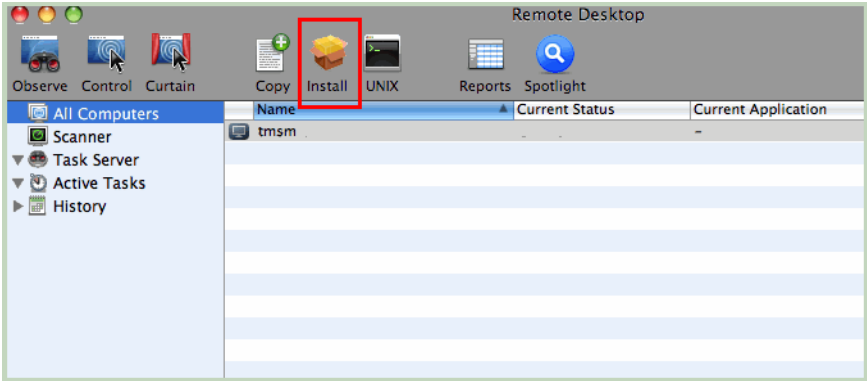


FIGURE E-15. Remote Desktop screen

- 6. On the Install Packages screen, drag the installation package or click "+" to locate the installation package.

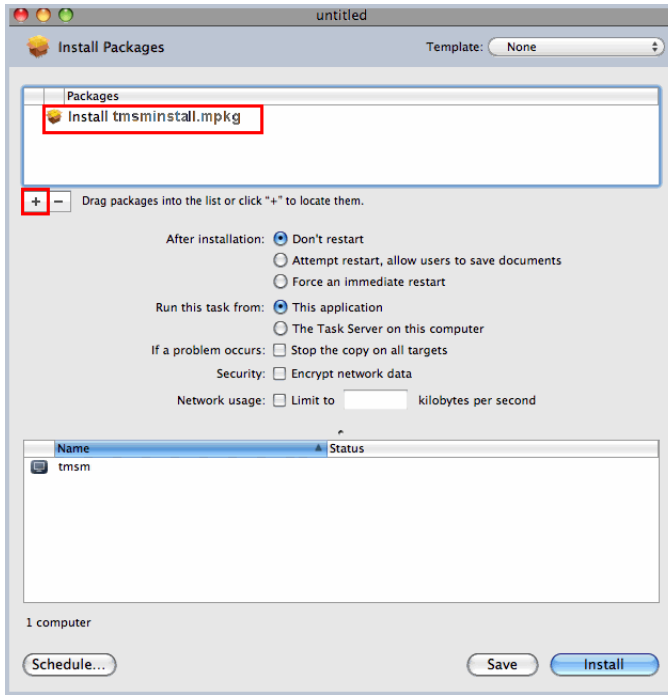


FIGURE E-16. Install Packages screen

7. (Optional) Click **Save** to automatically run the installation task on new Macintosh computers that connect to the network.
8. Click **Install**. The Apple Remote Desktop starts installing the client to the selected computers. If the installation was successful on all computers, the message **Install Packages: Succeeded on all** appears. Otherwise, **Successful** appears under **Task Status** for each computer to which the installation was successful.

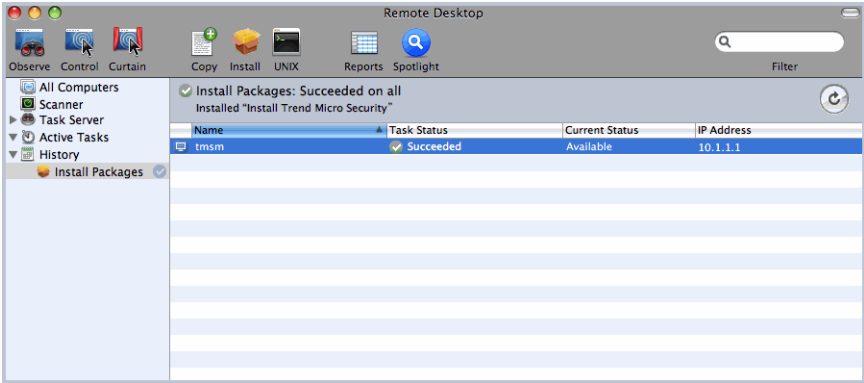


FIGURE E-17. Successful Installation screen

Clients automatically register to the server where the client installation package was obtained. Clients also update for the first time.

9. Perform client postinstallation tasks (See [Client Postinstallation](#) on page E-29).

Client Postinstallation

Perform the following tasks immediately after installing the Trend Micro Security client:

1. Verify the following:
 - The Trend Micro Security client icon displays on the menu bar of the Macintosh computer.
- 
- The Trend Micro Security client files are found under the {Client installation folder}.
 - The client appears on the Web Console’s client tree. To access the client tree, click **Client Management** on the main menu.

2. Update Trend Micro Security components. The client downloads components from the Trend Micro Security Server. See [Client Update](#) on page E-37.

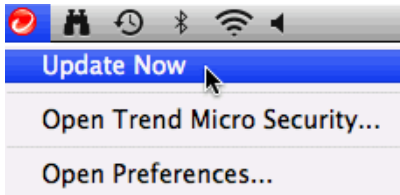


FIGURE E-18. Update Now menu item

If the client cannot connect to the server, it downloads directly from the Trend Micro ActiveUpdate server. Internet connection is required to connect to the ActiveUpdate server.

3. Initiate Scan Now (see [Scan Now](#) on page E-45) on the client computer or instruct the user to run Manual Scan.

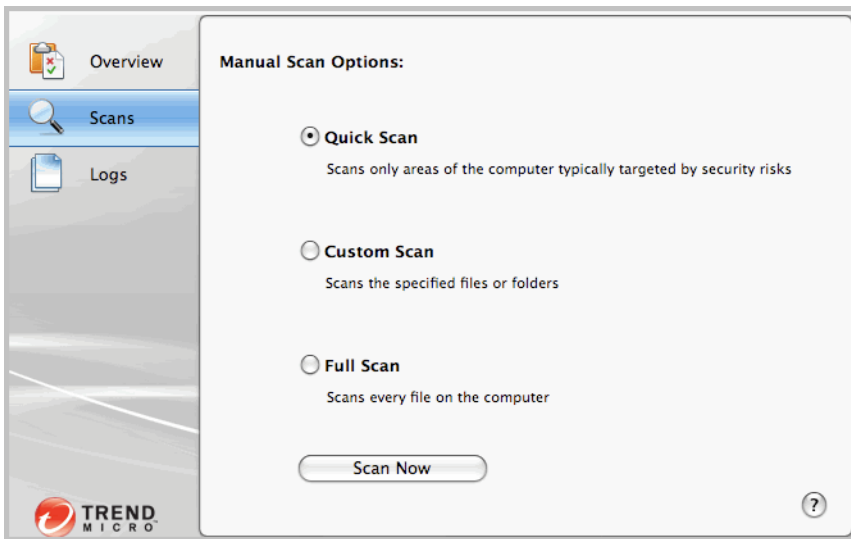


FIGURE E-19. Manual Scan screen on the endpoint

4. If there are problems with the client after installation, try uninstalling and then reinstalling the client.

Client Uninstallation

Uninstall the client program only if you encounter problems with the program. Reinstall it immediately to keep the computer protected from security risks.

To uninstall the client:

1. Obtain the client uninstallation package `tmsmuninstall.mpkg.zip` from the Trend Micro Security Server. On the Web Console, navigate to **Administration > Client Setup Files** and click the link under **Client Uninstallation File**.
2. Copy and then launch the package on the Macintosh computer.
3. Fill in the **Name** and **Password** fields to begin the uninstallation process.

Note: Specify the name and password for an account with administrative rights on the Macintosh computer.

4. If the uninstallation was successful, click **Close** to finish the uninstallation process.
5. Unregister the client from the server.
 - a. On the Web Console, click **Client Management** and select the client that was uninstalled.
 - b. Click **Manage Client Tree > Remove Group/Client**.

Keeping Protection Up-to-Date

Components

Trend Micro Security makes use of components to keep client computers protected from the latest security risks. Keep these components up-to-date by running manual or scheduled updates.

In addition to the components, Trend Micro Security clients also receive updated configuration files from the Trend Micro Security Server. Clients need the configuration files to apply new settings. Each time you modify Trend Micro Security settings through the Web Console, the configuration files change.

Virus Pattern

The Virus Pattern contains information that helps Trend Micro Security identify the latest virus/malware and mixed threat attack. Trend Micro creates and releases new versions of the Virus Pattern several times a week, and any time after the discovery of a particularly damaging virus/malware.

Spyware/Grayware Pattern

The Spyware/Grayware Pattern contains information that helps Trend Micro Security identify spyware and grayware.

Virus Scan Engine

At the heart of all Trend Micro products lies the scan engine, which was originally developed in response to early file-based computer viruses. The scan engine today is exceptionally sophisticated and capable of detecting different types of security risks, including spyware. The scan engine also detects controlled viruses that are developed and used for research.

Updating the Scan Engine

By storing the most time-sensitive information about security risks in the pattern files, Trend Micro minimizes the number of scan engine updates while keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. Trend Micro releases new engines under the following circumstances:

- Incorporation of new scanning and detection technologies into the software
- Discovery of a new, potentially harmful security risk that the scan engine cannot handle
- Enhancement of the scanning performance
- Addition of file formats, scripting languages, encoding, and/or compression formats

Client Program

The Trend Micro Security client program provides the actual protection from security risks.

Update Overview

All component updates originate from the Trend Micro ActiveUpdate server. When updates are available, the Trend Micro Security Server downloads the updated components.

You can configure the Trend Micro Security Server to update from a source other than the Trend Micro ActiveUpdate server. To do this, you need to set up a custom update source. For assistance in setting up this update source, contact your support provider.

The following table describes the different component update options for the Trend Micro Security Server and clients:

TABLE E-5. Server-client update options

UPDATE OPTION	DESCRIPTION
ActiveUpdate server Trend Micro Security Server Clients	The Trend Micro Security Server receives updated components from the Trend Micro ActiveUpdate server (or another update source if a custom source has been set up) and then deploys the components to clients.
ActiveUpdate server Clients	Trend Micro Security clients receive updated components directly from the ActiveUpdate server if they cannot connect to the Trend Micro Security Server.

Server Update

The Trend Micro Security Server downloads the following components and deploys them to clients:

- [Virus Pattern](#) on page E-32
- [Spyware/Grayware Pattern](#) on page E-32
- [Virus Scan Engine](#) on page E-32

View the current versions of components on the Web Console's Summary screen, and determine the number of clients with updated and outdated components.

If you use a proxy server to connect to the Internet, use the correct proxy settings to download updates successfully.

Server Update Source

Navigation Path: **Server Updates > Update Source**

Configure the Trend Micro Security Server to download components from the Trend Micro ActiveUpdate server or from another source.

After the server downloads any available updates, it automatically notifies clients to update their components. If the component update is critical, let the server notify the clients at once by navigating to **Client Management > Tasks > Update**.

To configure the server update source:

1. Select the location from which to download component updates.

If you choose ActiveUpdate server, ensure that the server is connected to the Internet and, if you are using a proxy server, verify that the Internet connection can be established using the proxy settings. See [Proxy for Server Update](#) on page E-35.

If you choose a custom update source, set up the appropriate environment and update resources for this update source. Ensure that there is a functional connection between the server computer and this update source. For assistance in setting up an update source, contact your support provider.

2. Click **Save**.

Proxy for Server Update

Navigation Path: **Administration > External Proxy Settings**

Configure the Trend Micro Security Server to use proxy settings when downloading updates from the Trend Micro ActiveUpdate server.

To configure proxy settings:

1. Select **Use the following proxy settings for pattern, engine, and license updates**.
2. Select the proxy protocol.
3. Type the proxy server name or IP address and the port number.
4. If the proxy server requires authentication, type the user name and password in the fields provided.
5. Click **Save**.

Server Update Methods

Update Trend Micro Security Server components manually or by configuring an update schedule.

Manual Update

When an update is critical, perform manual update so the server can obtain the updates immediately. See [Manual Update](#) on page E-37.

Scheduled Update

The Trend Micro Security Server connects to the update source during the scheduled day and time to obtain the latest components. See [Scheduled Update](#) on page E-36.

Scheduled Update

Navigation Path: Server Updates > Scheduled Update

Configure the Trend Micro Security Server to regularly check its update source and automatically download any available updates. Using scheduled update is an easy and effective way of ensuring that protection against security risks is always current.

To configure server update schedule:

1. Select the components to update.
2. Specify the update schedule by doing one of the following:
 - Select **Hourly** and click **Save**. Trend Micro Security will update the components hourly.
 - Select daily, weekly, or monthly updates (including the day of the month on which to update) and select a start time. In **Update for a period of** select the number of hours during which Trend Micro Security will perform the update. Trend Micro Security updates at any given time during this time period, which begins at the start time that you set.
3. Click **Save**.

Manual Update

Navigation Path: Server Updates > Manual Update

Manually update the components on the Trend Micro Security Server after installing or upgrading the server and whenever there is an outbreak.

To update the server manually:

1. Select the components to update.
2. Click **Update**. The server downloads the updated components.

Client Update

To ensure that clients stay protected from the latest security risks, update client components regularly. Also update clients with severely out-of-date components and whenever there is an outbreak. Components become severely out-of-date when the client is unable to update from the Trend Micro Security Server or the ActiveUpdate server for an extended period of time.

In addition to components, Trend Micro Security clients also receive updated configuration files during updates. Clients need the configuration files to apply new settings. Each time you modify Trend Micro Security settings on the Web Console, the configuration files change.

Before updating the clients, check if the Trend Micro Security Server has the latest components. For information on how to update the Trend Micro Security Server, see [Server Update](#) on page E-34.

Note: Trend Micro Security clients can use proxy settings during an update. Proxy settings are configured on the client console.

There are several ways to update clients.

- **Server-initiated update:** You can initiate an update from the Web Console by navigating to **Client Management > Tasks > Update**.
- **Automatic update:** After the server finishes an update, it immediately notifies clients to update.
- **Manual update:** Users launch the update from their Macintosh computers.

During an update, The Trend Micro Security icon on the menu bar of the Macintosh computer indicates that the product is updating. If an upgrade to the client program is available, clients update and then upgrade to the latest program version or build. Users cannot run any task from the console until the update is complete.

Access the **Summary** screen to check if all clients have been updated.

Protecting Computers from Security Risks

About Security Risks

Security risk includes viruses, malware, spyware, and grayware. Trend Micro Security protects computers from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak, which Trend Micro Security can help contain by enforcing outbreak prevention policies and isolating infected computers until they are completely risk-free. Notifications and logs help you keep track of security risks and alert you if you need to take immediate action.

Viruses and Malware

Tens of thousands of virus/malware exist, with more being created each day. Computer viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and websites.

Trend Micro Security protects computers from the following virus/malware types:

TABLE E-6. Viruses and malware types

VIRUS OR MALWARE TYPE	DESCRIPTION
Joke Program	A joke program is a virus-like program that often manipulates the appearance of things on a computer monitor.
Trojan Horse Program	A Trojan horse is an executable program that does not replicate but instead resides on computers to perform malicious acts, such as opening ports for hackers to enter. This program often uses Trojan Ports (see <i>Trojan Ports</i> on page 6-18) to gain access to computers. An application that claims to rid a computer of viruses when it actually introduces viruses to the computer is an example of a Trojan program. Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those already running on the system.
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. • Boot sector virus: A virus that infects the boot sector of a partition or a disk. • Java malicious code: Operating system-independent virus code written or embedded in Java™. • Macro virus: A virus encoded as an application macro and often included in a document. • VBScript, JavaScript, or HTML virus: A virus that resides on web pages and downloads through a browser. • Worm: A self-contained program or set of programs able to spread functional copies of itself or its segments to other computers, often through email

TABLE E-6. Viruses and malware types (Continued)

VIRUS OR MALWARE TYPE	DESCRIPTION
Test Virus	A test virus is an inert file that is detectable by virus scanning software. Use test viruses, such as the EICAR test script, to verify that the antivirus installation scans properly.
Packer	Packers are compressed and/or encrypted Windows or Linux™ executable programs, often a Trojan horse program. Compressing executables makes packers more difficult for antivirus products to detect.
Probable Virus/Malware	Suspicious files that have some of the characteristics of virus/malware are categorized under this virus/malware type. For details about probable virus/malware, see the following page on the Trend Micro online Virus Encyclopedia: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS
Others	"Others" include viruses/malware not categorized under any of the virus/malware types.

Spyware and Grayware

Spyware and grayware refer to applications or files not classified as viruses or malware, but can still negatively affect the performance of the computers on the network.

Spyware and grayware introduce significant security, confidentiality, and legal risks to an organization. Spyware/Grayware often performs a variety of undesired and threatening actions such as irritating users with pop-up windows, logging user keystrokes, and exposing computer vulnerabilities to attack.

Trend Micro Security protects computers from the following spyware/grayware types:

TABLE E-7. Spyware/Grayware types

SPYWARE/ GRAYWARE TYPES	DESCRIPTION
Spyware	Spyware gathers data, such as account user names, passwords, credit card numbers, and other confidential information, and transmits it to third parties.
Adware	Adware displays advertisements and gathers data, such as web surfing preferences, used for targeting future advertising at the user.
Dialer	A dialer changes client Internet settings and can force a computer to dial preconfigured phone numbers through a modem. These are often pay-per-call or international numbers that can result in a significant expense for an organization.
Hacking Tool	A hacking tool helps hackers enter a computer.
Remote Access Tool	A remote access tool helps hackers remotely access and control a computer.
Password Cracking Application	This type of application helps decipher account user names and passwords.
Others	"Others" include potentially malicious programs not categorized under any of the spyware/grayware types.

Scan Types

Trend Micro Security provides the following scan types to protect client computers from security risks:

TABLE E-8. Scan types

SCAN TYPE	DESCRIPTION
Real-time Scan	Automatically scans a file on the computer as it is received, opened, downloaded, copied, or modified See <i>Real-Time Scan</i> on page E-42.
Manual Scan	A user-initiated scan that scans a file or a set of files requested by the user See <i>Manual Scan</i> on page E-43.
Scheduled Scan	Automatically scans files on the computer based on the schedule configured by the administrator See <i>Scheduled Scan</i> on page E-44.
Scan Now	An administrator-initiated scan that scans files on one or several target computers See <i>Scan Now</i> on page E-45.

Real-Time Scan

Navigation Path: Client Management > Settings > Real-time Scan Settings

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If Trend Micro Security does not detect a security risk, the file remains in its location and users can proceed to access the file. If Trend Micro Security detects a security risk, it displays a notification message, showing the name of the infected file and the specific security risk.

Configure and apply Real-time Scan settings to one or several clients and groups, or to all clients that the server manages.

To configure Real-time Scan settings:

1. Select **Enable Real-time Scan**.
2. Configure the following scan criteria:
 - User Activity on Files that will trigger Real-time Scan (See [User Activity on Files](#) on page E-45)
 - [Scan Settings](#) on page E-46
3. Click the **Action** tab to configure the scan actions ([Scan Actions](#) on page E-48) for Trend Micro Security to perform on detected security risks.
4. If you selected group(s) or client(s) on the client tree, click **Save** to apply settings to the group(s) or client(s). If you selected the root icon , choose from the following options:
 - **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing or future group. Future groups are groups not yet created at the time you configure the settings.
 - **Apply to Future Groups Only:** Applies settings only to clients added to future groups. This option will not apply settings to new clients added to an existing group.

Manual Scan

Navigation Path: Client Management > Settings > Manual Scan Settings

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the client console. The time it takes to complete scanning depends on the number of files to scan and the client computer's hardware resources.

Configure and apply Manual Scan settings to one or several clients and groups, or to all clients that the server manages.

To configure Manual Scan settings:

1. On the **Target** tab, configure the following scan criteria:
 - [Scan Settings](#) on page E-46
 - [CPU Usage](#) on page E-47
2. Click the **Action** tab to configure the scan actions ([Scan Actions](#) on page E-48) for Trend Micro Security to perform on detected security risks.

3. If you selected group(s) or client(s) on the client tree, click **Save** to apply settings to the group(s) or client(s). If you selected the root icon  , choose from the following options:
 - **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing or future group. Future groups are groups not yet created at the time you configure the settings.
 - **Apply to Future Groups Only:** Applies settings only to clients added to future groups. This option will not apply settings to new clients added to an existing group.

Scheduled Scan

Navigation Path: Client Management > Settings > Scheduled Scan Settings

Scheduled Scan runs automatically on the appointed date and time. Use Scheduled Scan to automate routine scans on the client and improve scan management efficiency.

Configure and apply Scheduled Scan settings to one or several clients and groups, or to all clients that the server manages.

To configure Scheduled Scan settings:

1. Select **Enable Scheduled Scan**.
2. Configure the following scan criteria:
 - *Schedule* on page E-47
 - *Scan Target* on page E-46
 - *Scan Settings* on page E-46
 - *CPU Usage* on page E-47
3. Click the **Action** tab to configure the *scan actions* Trend Micro Security performs on detected security risks.
4. If you selected group(s) or client(s) on the client tree, click **Save** to apply settings to the group(s) or client(s). If you selected the root icon  , choose from the following options:

- **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing or future group. Future groups are groups not yet created at the time you configure the settings.
- **Apply to Future Groups Only:** Applies settings only to clients added to future groups. This option will not apply settings to new clients added to an existing group.

Scan Now

Scan Now is initiated remotely by a Trend Micro Security administrator through the Web Console and can be run on one or several client computers.

Initiate Scan Now on computers that you suspect to be infected. To initiate Scan Now, navigate to **Client Management > Tasks > Scan Now**.

All the Scheduled Scan Settings, except the actual schedule, are used during Scan Now (See *Scheduled Scan* on page E-44).

Settings Common to All Scan Types

For each scan type, configure three sets of settings:

- *Scan Criteria* on page E-45
- *Scan Exclusions* on page E-48
- *Scan Actions* on page E-48

Deploy these settings to one or several clients and groups, or to all clients that the server manages.

Scan Criteria

Specify which files a particular scan type should scan using file attributes such as file type and extension. Also specify conditions that will trigger scanning. For example, configure Real-time Scan to scan each file after it is downloaded to the computer.

User Activity on Files

Choose activities on files that will trigger Real-time Scan. Select from the following options:

- **Scan files being created/modified:** Scans new files introduced into the computer (for example, after downloading a file) or files being modified
- **Scan files being retrieved/executed:** Scans files as they are opened
- Scan files being created/modified and retrieved/executed

For example, if the third option is selected, a new file downloaded to the computer will be scanned and stays in its current location if no security risk is detected. The same file will be scanned when a user opens the file and, if the user modified the file, before the modifications are saved.

Scan Target

Select from the following options.

- **All scannable files:** Scan all files
- **File types scanned by IntelliScan:** Only scan files known to potentially harbor malicious code, including files disguised by a harmless extension name. See [IntelliScan](#) on page D-4.
- **File or folder name with full path:** Only scan the specified file or files found in a specific folder.

Scan Settings

Trend Micro Security can scan individual files within compressed files. Trend Micro Security supports the following compression types:

TABLE E-9. Supported compressed files

EXTENSION	TYPE
.zip	Archive created by Pkzip
.rar	Archive created by RAR
.tar	Archive created by Tar
.arj	ARJ Compressed archive
.hqx	BINHEX
.gz; .gzip	Gnu ZIP

TABLE E-9. Supported compressed files (Continued)

EXTENSION	TYPE
.Z	LZW/Compressed 16bits
.bin	Mac Binary
.cab	Microsoft™ Cabinet file
Microsoft™ Compressed/MSCOM P	
.eml; .mht	MIME
.td0	Teledisk format
.bz2	Unix BZ2 Bzip compressed file
.uu	UUEncode
.ace	WinAce

CPU Usage

Trend Micro Security can pause after scanning one file and before scanning the next file. This setting is used during Manual Scan, Scheduled Scan, and Scan Now.

Select from the following options:

- **High:** No pausing between scans
- **Low:** Pause between file scans

Schedule

Configure how often and what time Scheduled Scan will run. Select from the following options and then select the start time:

- Daily
- Weekly
- Monthly

Scan Exclusions

Configure scan exclusions to increase the scanning performance and skip scanning files that are known to be harmless. When a particular scan type runs, Trend Micro Security checks the scan exclusion list to determine which files on the computer will be excluded from scanning.

When you enable scan exclusion, Trend Micro Security will not scan a file under the following conditions:

- The file name matches any of the names in the exclusion list.
- The file extension matches any of the extensions in the exclusion list.

Scan Exclusion List (Files)

Trend Micro Security will not scan a file if its file name matches any of the names included in this exclusion list. If you want to exclude a file found under a specific location on the computer, include the file path, such as
`\Users\tmsm\Desktop\test.ppt .`

You can specify a maximum of 64 files.

Scan Exclusion List (File Extensions)

Trend Micro Security will not scan a file if its file extension matches any of the extensions included in this exclusion list. You can specify a maximum of 64 file extensions. A period (.) is not required before the extension.

Scan Actions

Specify the action Trend Micro Security performs when a particular scan type detects a security risk.

The action Trend Micro Security performs depends on the scan type that detected the security risk. For example, when Trend Micro Security detects a security risk during Manual Scan (scan type), it cleans (action) the infected file.

Actions

The following are the actions Trend Micro Security can perform against security risks:

Delete

Trend Micro Security removes the infected file from the computer.

Quarantine

Trend Micro Security renames and then moves the infected file to the quarantine directory on the client computer located in
`{Client installation folder}/common/lib/vsapi/quarantine.`

Once in the quarantine directory, Trend Micro Security can perform another action on the quarantined file, depending on the action specified by the user. Trend Micro Security can delete, clean, or restore the file. Restoring a file means moving it back to its original location without performing any action. Users may restore the file if it is actually harmless. Cleaning a file means removing the security risk from the quarantined file and then moving it to its original location if cleaning is successful.

Clean

Trend Micro Security removes the security risk from an infected file before allowing users to access it.

If the file is uncleanable, Trend Micro Security performs a second action, which can be one of the following actions: Quarantine, Delete, and Pass. To configure the second action, navigate to **Client Management > Settings > {Scan Type} > Action** tab.

Pass

Trend Micro Security performs no action on the infected file but records the detected security risk in the logs. The file stays where it is located.

Trend Micro Security always performs "Pass" on files infected with the probable virus/malware type to mitigate a false positive (See *Probable Virus/Malware* on page E-40). If further analysis confirms that probable virus/malware is indeed a security risk, a new pattern will be released to allow Trend Micro Security to perform the appropriate scan action. If actually harmless, probable virus/malware will no longer be detected.

For example:

Trend Micro Security detects "x_probable_virus" on a file named 123.pdf and performs no action at the time of detection. Trend Micro then confirms that "x_probable_virus" is a Trojan horse program and releases a new Virus Pattern version. After loading the new pattern, Trend Micro Security will detect "x_probable_virus" as a Trojan program and, if the action against such programs is "Delete", will delete 123.pdf.

Scan Action Options

When configuring the scan action, select from the following options:

Use **ActiveAction**

ActiveAction is a set of preconfigured scan actions for different types of security risks. If you are unsure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction.

ActiveAction settings are constantly updated in the pattern files to protect computers against the latest security risks and the latest methods of attacks.

Use the same action for all security risk types

Select this option if you want the same action performed on all types of security risks, except probable virus/malware. For probable virus/malware, the action is always "Pass" (See *Probable Virus/Malware* on page E-40).

If you choose "Clean" as the first action, select a second action that Trend Micro Security performs if cleaning is unsuccessful. If the first action is not "Clean," no second action is configurable.

Display a Notification Message When a Security Risk is Detected

When Trend Micro Security detects a security risk during Real-time Scan, it can display a notification message to inform the user about the detection.

Allow Users to Postpone or Cancel Scheduled Scan

Trend Micro Security displays a notification message five minutes before Scheduled Scan runs. Users can postpone scanning to a later time and will be reminded again before the scan runs. Users can also cancel the scan.

Security Risk Notifications

Trend Micro Security comes with a set of default notification messages to inform you and other Trend Micro Security administrators of detected security risks or any outbreak that has occurred.

Administrator Notification Settings

Navigation Path: Notifications > General Settings

When security risks are detected or when an outbreak occurs, Trend Micro Security administrators can receive notifications through email.

To configure administrator notification settings:

Specify information in the fields provided.

1. In the **SMTP server** field, type either an IP address or computer name.
 - a. Type a port number between 1 and 65535.
 - b. Type the sender's email address in the **From** field.
2. Click **Save**.

Security Risk Notifications for Administrators

Navigation Path: Notifications > Standard Notifications

Configure Trend Micro Security to send a notification when it detects a security risk, or only when the action on the security risk is unsuccessful and therefore requires your intervention.

You can receive notifications through email. Configure administrator notification settings to allow Trend Micro Security to successfully send notifications through email. See [Administrator Notification Settings](#) on page E-51.

To configure security risk notifications for administrators:

1. In the **Criteria** tab, specify whether to send notifications each time Trend Micro Security detects a security risk, or only when the action on the security risks is unsuccessful.
2. Click **Save**.

3. In the **Email** tab:

- Enable notifications to be sent through email.
- Specify the email recipients and accept or modify the default subject.

Token variables are used to represent data in the **Message** field.

TABLE E-10. Token variables for security risk notifications

VARIABLE	DESCRIPTION
%v	Security risk name
%s	The computer where the security risk was detected
%m	Client tree group to which the computer belongs
%p	Location of the security risk
%y	Date and time of detection

4. Click **Save**.

Outbreak Criteria and Notifications for Administrators

Navigation Path: Notifications > Outbreak Notifications

Define an outbreak by the number of security risk detections and the detection period. After defining the outbreak criteria, configure Trend Micro Security to notify you and other Trend Micro Security administrators of an outbreak so you can respond immediately.

You can receive notifications through email. Configure administrator notification settings to allow Trend Micro Security to successfully send notifications through email. See [Administrator Notification Settings](#) on page E-51.

To configure the outbreak criteria and notifications:

1. In the **Criteria** tab, specify the following:
 - Number of unique sources of security risks, if any
 - Number of detections

- Detection period

Tip: Trend Micro recommends accepting the default values in this screen.

Trend Micro Security declares an outbreak and sends a notification message when the number of detections is exceeded. For example, if you specify 100 detections, Trend Micro Security sends the notification after it detects the 101st instance of a security risk.

2. Click **Save**.
3. In the **Email** tab:
 - a. Enable notifications to be sent through email.
 - b. Specify the email recipients and accept or modify the default subject.

Token variables are used to represent data in the **Message** field.

TABLE E-11. Token variables for outbreak notifications

VARIABLE	DESCRIPTION
%CV	Total number of security risks detected
%CC	Total number of computers with security risks

4. Select additional information to include in the email. You can include the client/group name, security risk name, path and affected file, date and time of detection, and scan result.
5. Click **Save**.

Security Risk Logs

Navigation Path: Client Management > Logs > Security Risk Logs

Trend Micro Security generates logs when it detects security risks. To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see [Managing Logs](#) on page E-63.

To view security risk logs:

1. Specify the log criteria and click **Display Logs**. The Security Risk Logs screen displays.
2. View logs. Logs contain the following information:
 - Date and time of security risk detection
 - Computer with security risk
 - Security risk name
 - Security risk source
 - Scan type that detected the security risk
 - Scan Results (page E-55), which indicate whether scan actions were performed successfully
 - Platform
3. To save logs to a comma-separated value (CSV) file, click **Export**. Open the file or save it to a specific location. If you are exporting a large number of logs, wait for the export task to finish. If you close the page before the export task is finished, the .csv file will not be generated.

Scan Results

Security risk logs indicate any of the following scan results:

A. If Scan Action is Successful

The following results display if Trend Micro Security was able to perform the configured scan action:

Deleted

The first action is Delete (page E-49) and the infected file was deleted.

The first action is Clean (page E-49) but cleaning was unsuccessful. The second action is Delete and the infected file was deleted.

Quarantined

The first action is Quarantine (page E-49) and the infected file was quarantined.

The first action is Clean but cleaning was unsuccessful. The second action is Quarantine and the infected file was quarantined.

Cleaned

An infected file was cleaned.

Passed

The first action is [Pass](#) (page E-49). Trend Micro Security did not perform any action on the infected file.

The first action is Clean but cleaning was unsuccessful. The second action is Pass so Trend Micro Security did not perform any action on the infected file.

B. If Scan Action is Unsuccessful

The following results display if Trend Micro Security was unable to perform the configured scan action:

Unable to clean or quarantine the file

Clean is the first action, Quarantine is the second action, and both actions were unsuccessful.

Solution: See "Unable to quarantine the file" below.

Unable to clean or delete the file

Clean is the first action, Delete is the second action, and both actions were unsuccessful.

Solution: See "Unable to delete the file" below.

Unable to quarantine the file

The infected file may be locked by another application, is executing, or is on a CD. Trend Micro Security will quarantine the file after the application releases the file or after it has been executed.

Solution: For infected files on a CD, consider not using the CD as the security risk may spread other computers on the network.

Unable to delete the file

The infected file may be locked by another application, is executing, or is on a CD. Trend Micro Security will delete the file after the application releases the file or after it has been executed.

Solution: For infected files on a CD, consider not using the CD as the security risk may spread to other computers on the network.

Unable to clean the file

The file may be uncleanable (See [Uncleanable Files](#) on page 6-16).

About Web Threats

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, web threat creators constantly change the version or variant used. Because the web threat is in a fixed location of a website rather than on an infected computer, the web threat creator constantly modifies its code to avoid detection.

In recent years, individuals once characterized as hackers, virus writers, spammers, and spyware makers are now known as cyber criminals. Web threats help these individuals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is leakage of confidential information in the form of identity loss. The infected computer may also become a vector to deliver phishing attack or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in web commerce, corrupting the trust needed for Internet transactions. The second goal is to hijack a user's CPU power to use it as an instrument to conduct profitable activities. Activities include sending spam or conducting extortion in the form of distributed denial-of-service attacks or pay-per-click activities.

Web Reputation

Trend Micro Security leverages Trend Micro's extensive web security databases to check the reputation of websites that users are attempting to access. The website's reputation is correlated with the specific web reputation policy enforced on the computer. Depending on the policy in use, Trend Micro Security will either block or allow access to the website. Policies are enforced based on the client's location.

Web Reputation Policies

Navigation Path: Client Management > Settings > Web Reputation Settings

Web reputation policies dictate whether Trend Micro Security will block or allow access to a website. To determine the appropriate policy to use, Trend Micro Security checks the client's location. A client's location is "internal" if it can connect to the Trend Micro Security Server. Otherwise, a client's location is "external".

To configure a web reputation policy for external and internal clients:

1. Select **Enable Web Reputation Policy**.
2. Select from the available web reputation security levels: High, Medium, or Low
3. For internal clients, in the Intern Clients tab Client Log section, select **Allow clients to send logs to the Trend Micro Security (for Mac) server**, or leave the box empty. Allow clients to send Web Reputation Logs (page E-59) if you want to analyze URLs being blocked by Trend Micro Security and take the appropriate action on URLs that you think are safe to access.
4. If you selected group(s) or client(s) on the client tree, click **Save** to apply settings to the group(s) or client(s). If you selected the root icon , choose from the following options:
 - **Apply to All Clients:** Applies settings to all existing clients and to any new client added to an existing or future group. Future groups are groups not yet created at the time you configure the settings.
 - **Apply to Future Groups Only:** Applies settings only to clients added to future groups. This option will not apply settings to new clients added to an existing group.

Security Levels

The security levels (High, Medium, or Low) determine whether Trend Micro Security allows or blocks access to a URL. For example, if you set the security level to "Low," Trend Micro Security only blocks URLs that are known to be web threats. As you set the security level higher, the web threat detection rate improves but the possibility of false positives also increases.

Approved URLs

Navigation Path: Administration > Web Reputation Approved URL List

Approved URLs bypass Web Reputation policies. Trend Micro Security does not block these URLs even if the Web Reputation policy is set to block them. Add URLs that you consider safe to the approved URL list.

To configure the approved URL list:

1. Type a URL in the text box. You can add a wildcard character (*) anywhere on the URL.

Examples:

- www.trendmicro.com/* means that all pages under www.trendmicro.com will be approved.
- *.trendmicro.com/* means that all pages on any sub-domain of trendmicro.com will be approved.

2. Click **Add**.
3. To delete an entry, click the delete icon () to the right of an approved URL.
4. Click **Save**.

Web Reputation Logs

Navigation Path: Client Management > Logs > Web Reputation Logs

Configure internal clients to send web reputation logs to the server. Do this if you want to analyze URLs that Trend Micro Security blocks and take appropriate action on URLs you think are safe to access.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule. For more information about managing logs, see [Managing Logs](#) on page E-63.

To view web reputation logs:

1. Specify the log criteria and click **Display Logs**.
2. View logs. Logs contain the following information:
 - **Date/Time** that Trend Micro Security blocked the URL
 - **Computer** where the user accessed the URL
 - The blocked **URL**
 - **Risk Level** of the URL
 - **Details:** A link to the Trend Micro Web Reputation Query system that provides more information about the blocked URL

3. To save logs to a comma-separated value (CSV) file, click **Export**. Open the file or save it to a specific location. If you are exporting a large number of logs, wait for the export task to finish. If you close the page before the export task is finished, the .csv file will not be generated.

Managing the Trend Micro Security Server and Clients

Upgrading the Server and Clients

The Plug-in Manager console displays any new Trend Micro Security build or version. Upgrade the server and clients immediately when the new build or version becomes available. Trend Micro Security only displays a Download button:

- When the plug-in has not yet been installed for the first time
- When an Trend Micro Security upgrade is available

To upgrade the server:

1. On the Worry-Free Business Security Web Console, click **Preferences > Plug-Ins**. The Plug-Ins screen appears.
2. In the **Trend Micro Security (for Mac)** section, click **Download**.

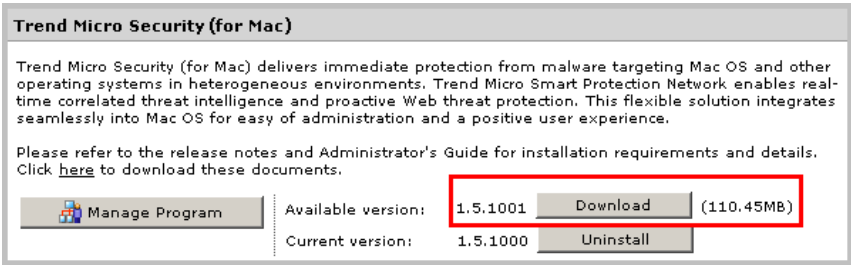


FIGURE E-20. Web Console displaying a new Trend Micro Security build

Note: Plug-in Manager downloads the package to {WFBS installation folder}\PCCSRV\Download\Product.

{WFBS server installation folder} is typically
C:\Program Files\Trend Micro\Security Server.

3. Monitor the download progress. You can navigate away from the screen during the download.

Note: If you encounter problems downloading the package, check the server update logs on the Worry-Free Business Security Web Console. On the main menu, click **Logs > Server Update Logs**.

4. After Plug-in Manager downloads the package, a new screen displays, providing you the following options: **Upgrade Now** or **Upgrade Later**.
5. If you choose to immediately upgrade, check the upgrade progress.
6. If you return to upgrade later:

- a. Open the Worry-Free Business Security Web Console and click **Preferences > Plug-Ins** on the main menu.
- b. In the **Trend Micro Security (for Mac)** section, click **Upgrade**.
- c. Check the upgrade progress.

After the upgrade, the Trend Micro Security version displays.

To upgrade clients:

1. Perform any of the following steps:
 - Perform a [manual update](#). Ensure that you select **Trend Micro Security Client** from the list of components.
 - On the client tree, select the clients to upgrade and then click **Tasks > Update**.
 - If [scheduled update](#) has been enabled, ensure that **Trend Micro Security Client** is selected.
 - Instruct users to click **Update Now** from the client console.

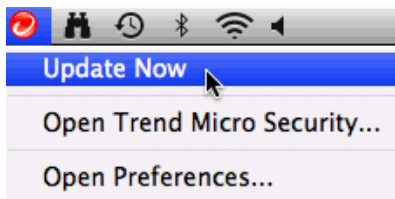


FIGURE E-21. Update Now menu item

Clients that receive the notification start to upgrade. On the Macintosh computer, the Trend Micro Security icon on the menu bar indicates that the product is updating. Users cannot run any task from the console until the upgrade is complete.

2. Check the upgrade status from the Trend Micro Security Summary screen by going to the **Update Status for Networked Computers** section.
 - In the Program section click the link in the **Not Upgraded** column. The client tree opens, showing all the clients that have not been upgraded.
 - To upgrade the clients, click **Tasks > Update**.

Managing Logs

Navigation Path: Administration > Log Maintenance

Trend Micro Security keeps comprehensive logs about security risk detections and blocked URLs. Use these logs to assess your organization's protection policies and to identify clients that are at a higher risk of infection or attack.

To keep the size of logs from occupying too much space on the hard disk, manually delete logs or configure a log deletion schedule from the Web Console.

To delete logs based on a schedule:

1. Select **Enable scheduled deletion of logs**.
2. Select whether to delete all logs or only logs older than a certain number of days.
3. Specify the log deletion frequency and time.
4. Click **Save**.

Licenses

Navigation Path: Administration > Product License

View, activate, and renew the Trend Micro Security license on the Web Console.

The status of the product license determines the features available to users. Refer to the table below for details.

TABLE E-12. License types and status

LICENSE TYPE AND STATUS	FEATURES			
	REAL-TIME SCAN	MANUAL/ SCHEDULED SCAN	WEB REPUTATION	PATTERN UPDATE
Full version and Activated	Enabled	Enabled	Enabled	Enabled
Evaluation (trial) version and Activated	Enabled	Enabled	Enabled	Enabled
Full version and Expired	Enabled	Enabled	Disabled	Disabled
Evaluation version and Expired	Disabled	Disabled	Disabled	Disabled
Not activated	Disabled	Disabled	Disabled	Disabled

To manage product licenses:

1. View license information. To get the latest license information, click **Update Information**.

The **License** section shows the following details:

- **Status:** Displays either "Activated" or "Expired"

- **Version:** Displays either "Full" or "Evaluation" version. If you are using an evaluation version, you can upgrade to the full version anytime. For upgrade instructions, click the **View license upgrade instructions** link.
 - **Seats:** The maximum number of client installations that the license supports
 - **License expires on:** The expiration date of the license
 - **Activation Code:** The code used to activate the license
 - **View detailed license online:** in the section title bar, a link to the Trend Micro website where you can view detailed information about your license
2. To specify a new Activation Code, click **New Activation Code**.
 3. In the screen that opens, type the **Activation Code** and click **Save**.

Client-Server Communication

Navigation Path: Administration > Client-Server Communication

Clients identify the server that manages them by the server's name or IP address. During the Trend Micro Security Server installation, the installer identifies the server computer's IP addresses, which are then displayed on the Web Console's Client-Server Communication screen.

The server communicates with clients through the listening port, which is port number 61617 by default.

If you change the port number, ensure that it is not currently in use to prevent conflicts with other applications and client-server communication issues.

If a firewall application is in use on the server computer, ensure that the firewall does not block client-server communication through the listening port. For example, if the Worry-Free Business Security client firewall has been enabled on the computer, add a policy exception that allows incoming and outgoing traffic through the listening port.

You can configure clients to connect to the server through a proxy server. A proxy server, however, is usually not required for client-server connections within the corporate network.

If you need to configure the server name/IP address, listening port, and proxy server settings, configure them before installing clients. If you have installed clients and then change any of these settings, clients will lose connection with the server and the only way to re-establish connection is to redeploy the clients.

To configure client-server communication settings:

1. Type one or more server names or IP addresses and the listening port number.

Note: If there are multiple entries in the **Server name (or IP address)** field, the client randomly selects an entry. Ensure that client-server connection can be established using all the entries.

2. Select whether clients connect to the server through a proxy server.
 - a. Select the proxy server protocol.
 - b. Type the proxy server name or IP address and the port number.
 - c. If the proxy server requires authentication, type the user name and password.
3. Click **Save**.
4. If you are prompted to restart Trend Micro Security services for the settings to take effect, perform the following steps:
 - a. Navigate to the {Server installation folder}.
 - b. Double-click `restart_TMSM.bat`. Wait until all the services have restarted.

Mac Client Icons

Icons in the client computer's system tray indicate the client's status and the task it is currently running.

TABLE E-13. Client icons

ICON	COLOR	DESCRIPTION
	Red	The client is up and running and is connected to its parent server. In addition, any of the following is true: • The product license has been activated. • The product license has been activated but has expired. Some client features will not be available if the license has expired. See Full version and Expired on page E-64 and Evaluation version and Expired on page E-64.
	Gray	The client is up and running but is disconnected from its parent server.
	Red	The client is scanning for security risks and is connected to its parent server.

TABLE E-13. Client icons (Continued)

ICON	COLOR	DESCRIPTION
	Gray	The client is scanning for security risks but is disconnected from its parent server. If the client detects security risks during scanning, it will send the scan results to the server only when the connection is restored.
	Red	The client is updating components from its parent server.
	Gray	The client is updating components from the Trend Micro ActiveUpdate server because it cannot connect to its parent server.
	Gray	This icon indicates any of the following conditions: - The client has been registered to its parent server but the product license has not been activated. Some client features will not be available if the license has not been activated. See <i>Not activated</i> on page E-64. - The client has not been registered to its parent server. The product license may or may not have been activated. If a client is not registered to its parent server: - Real-time Scan is enabled but the action on security risks is always "Pass". - Manual Scan, Scheduled Scan, web reputation, and pattern updates are disabled. - The client has been registered to its parent server. The product license is for an evaluation (trial) version of the product and has been activated. However, the evaluation version license has expired. Some client features will not be available if the license has expired. See <i>Evaluation version and Expired</i> on page E-64.

Troubleshooting and Support

Troubleshooting

Web Console Access

Problem:

The Web Console cannot be accessed.

Solutions:

Perform the following steps:

1. Check if the computer meets the requirements for installing and running Trend Micro Security Server. See [Server Installation Requirements](#) on page E-4.
2. Check if the following services have been started:
 - ActiveMQ for Trend Micro Security
 - Worry-Free Business Security Plug-in Manager
 - SQL Server (TMSM)
 - Trend Micro Security for (Mac)
3. Collect debug logs. Use 'error' or 'fail' as keyword when performing a search on the logs.
 - Installation logs: C:\TMSM*.log
 - General debug logs: {Server installation folder}\debug.log
 - Worry-Free Business Security debug logs: C:\Program Files\Trend Micro\Security Server\PCCSRV\Log\ofcdebug.log
 - If the file does not exist, enable debug logging. On the banner of the Worry-Free Business Security Web Console, click the first "m" in "Trend Micro", specify debug log settings, and click **Save**.
 - Reproduce the steps that led to the Web Console access problem.
 - Obtain the debug logs.
4. Check the Trend Micro Security registry keys by navigating to HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMSM.
5. Check the database files and registry keys.

- a. Check if the following files exist under C:\Program Files\Microsoft SQL Server\MSSQL.x\MSSQL\Data\:
 - db_TSM.mdf
 - db_TSM_log.LDF
 - b. Check if the Trend Micro Security database instance on the Microsoft SQL server registry key exists:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.x\MSSQLServer\CurrentVersion
6. Send the following to Trend Micro:
 - Registry files
 - Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL server\TSM.
 - Click **File > Export** and then save the registry key to a .reg file.
 - Server computer information
 - Operating system and version
 - Available disk space
 - Available RAM
 - Whether other plug-in programs, such as Intrusion Defense Firewall, is installed
7. Restart the Trend Micro Security services.
 - a. Navigate to the {Server installation folder}.
 - b. Double-click restart_TSM.bat. Wait until all the services have restarted.
8. The Trend Micro Security (for Mac) service should always be running. If this service is not running, there may be a problem with the ActiveMQ service.
 - a. Back up ActiveMQ data in C:\Program Files\Trend Micro\Security Server\Addon\TSM\apache-activemq\data*.*.
 - b. Delete the ActiveMQ data.

- c. Try to restart the Trend Micro Security (for Mac) service by double-clicking `restart_TMSM.bat`.
- d. Try to access the Web Console again to check if the access problem has been resolved.

Server Uninstallation

Problem:

The following message displays:

Unable to uninstall the plug-in program. The uninstallation command for the plug-in program is missing in the registry key.

Solution:

1. Open registry editor and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_Addon_Service_CompList_Version`.
2. Reset the value to `1.0.1000`.
3. Delete the plug-in program registry key; for example, `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS\OSCE_ADDON_XXXX`.
4. Restart the Worry-Free Business Security Plug-in Manager service.
5. Download, install, and then uninstall the plug-in program.

Client Installation

Problem:

The installation was unsuccessful. The installation package (`tmsminstall.mpkg.zip`) was launched using an archiving tool not built-in on the Mac or through an unsupported command (such as **unzip**) issued from a command-line tool, causing the extracted installation files to become corrupted.

Solution 1:

Remove the extracted folder (`tmsminstall.mpkg`) and then launch the installation package again using a built-in archiving tool such as Archive Utility.

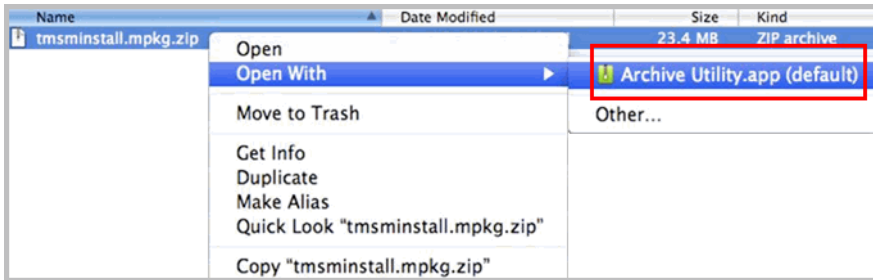


FIGURE E-22. Launching the package using Archive Utility

You can also launch the package from the command line by using the following command:

```
ditto -xk tmsminstall.mpkg.zip {destination folder}
```

Solution 2:

Set the correct permission to execute `tmsminstall.mpkg`.

1. Open the Terminal utility.
2. Change to the directory where `tmsminstall.mpkg` is located.
3. Type the following:

```
$ chmod +x  
tmsminstall.mpkg\Contents\Resources\integritycheck
```

4. Retry the installation.

Client Troubleshooting

Problem:

An error or problem was encountered on the client.

Solution:

Run the Trend Micro Security Debug Manager to collect data that may help resolve the error or problem.

To run the tool, open {Client installation folder}/Tools and launch **Trend Micro Debug Manager**. Follow the on-screen instructions in the tool to successfully collect data.

WARNING! The tool will not work if a user moves it to a different location on the Macintosh computer. If the tool has been moved, uninstall and then install the Trend Micro Security client.

If the tool was copied to another location, remove the copied version and then run the tool from its original location.

See *Getting Help* on page I-1.

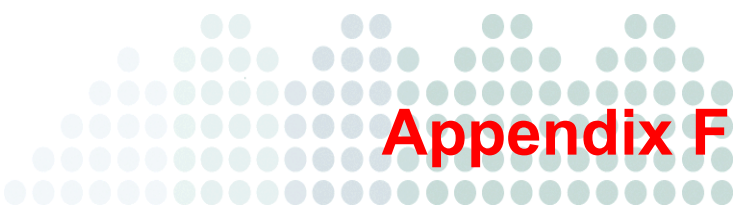
Security Information Center

Comprehensive security information is available at the Trend Micro website.

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

Information available:

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



Appendix F

TMSM Installation and Configuration Worksheet

This appendix provides a checklist of items to guide you in setting up and configuring Trend Micro™ Security *for Mac*. See [Trend Micro Security for Mac Plug-in](#) on page E-1 for detailed information on setup and configuration tasks.

Topics in this appendix:

- [Server Installation](#) on page F-2
- [Client Installation](#) on page F-5
- [Server Configuration](#) on page F-7

Server Installation

Before installing the Trend Micro Security Server, carefully review the items in this worksheet to speed up the installation of the server and avoid installation issues. Both the Worry-Free Business Security Server and the Plug-In Manager must already be installed before you can install the Trend Micro Security (for Mac) server. The system requirements in [Table F-1](#) below are for the Trend Micro Security Server only..

TABLE F-1. Trend Micro Security Server installation worksheet

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Computer name or IP address	--	
RAM	512MB minimum, 1GB recommended	
Available disk space	With Worry-Free™ Business Security Server installed on the system drive (usually, C: drive): • 1.5GB minimum Note: Trend Micro Security Server always installs on the same drive as the Worry-Free server. With Worry-Free server not installed on system drive: • 600MB minimum on the drive where the Worry-Free server is installed. • 900MB minimum on the system drive. Third-party programs used by Trend Micro Security Server (such as Microsoft SQL Server 2005 Express™) will be installed on this drive.	

TABLE F-1. Trend Micro Security Server installation worksheet (Continued)

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Other system requirements	• Microsoft™ .NET Framework 2.0 • Java runtime environment™ (JRE) 1.6 Update 14 or above on computers running Windows Server 2008	
Worry-Free Business Security Server	Version 7.0	
User name and password used to log on to the Worry-Free Business Security Server Web Console	Open the Web Console on the computer where the Worry-Free Business Security Server is installed. Trend Micro Security Server will not be installed successfully if you open the console on another computer and run the Trend Micro Security Server installation from there. Use an account with administrator privileges when logging on to the computer.	
Worry-Free Business Security Server installation folder	The default folder is C:\Program Files\Trend Micro\Security Server. Trend Micro Security installation files will be copied to C:\Program Files\Trend Micro\Security Server\Addon\TMSM. You cannot specify a different folder to which to copy the files.	
Plug-in Manager	Version 1.0 with the latest patch	

TABLE F-1. Trend Micro Security Server installation worksheet (Continued)

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Update source (Trend Micro ActiveUpdate server or custom update source)	• Internet connection is required if the update source is the Trend Micro ActiveUpdate server. Include proxy settings if connecting through a proxy server. • The following items are required if the update source is a custom update source: • Latest version of OSCE_AOS_COMP_LIST.xml • Trend Micro Security installation package	
Activation Code for an evaluation or full version license	Valid Activation Code with 31 alphanumeric characters specified in the following format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX	
Number of seats for the Activation Code	--	

Client Installation

Before installing the Trend Micro Security client, carefully review the items in this worksheet to speed up the installation of the client and avoid installation issues.

TABLE F-2. Client installation worksheet

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Computer name or IP address	--	
Operating system	• Mac OS™ X Snow Leopard™ 10.6 or later • Mac OS X version 10.5.6 (Leopard™) or later • Mac OS X version 10.4.11 (Tiger™) or later • Mac OS X Server	
Processor	PowerPC™ or Intel™ core processor	
RAM	256MB minimum	
Available disk space	30MB minimum	
Others	• Java for Mac OS X 10.4, Release 9 • Java for Mac OS X 10.5, Update 4	
Client-server communication settings (configured on the Trend Micro Security Server Web Console)	• Trend Micro Security Server name or IP address • Listening port (the default port is 61617) • (Optional) Proxy settings	

TABLE F-2. Client installation worksheet (Continued)

INSTALLATION ITEM	REQUIREMENTS/ RECOMMENDATIONS/NOTES	YOUR INFORMATION
Client installation package	To obtain the package, open the Trend Micro Security Server Web Console, navigate to Administration > Client Setup Files , and click the link under Client Installation File .	
Launching the installation package	The files on the package may become corrupted if users launch the package using archiving tools not built-in on the Mac. Instruct users to launch the package using built-in archiving tools, such as Archive Utility. Users can also launch the package from the command line by using the following command: <pre>ditto -xk tmsminstall.mpkg.zip {destination folder}</pre>	
Firewall in use in the server computer	The firewall should not block client-server communication through the listening port.	
Personal firewall in Mac OS X	If the personal firewall option Set access for specific services and applications is enabled, instruct users to allow connections to icorepluginMgr when prompted by the system. icorepluginMgr is used to register the client to the server.	

Server Configuration

The default settings that ship with this product should be able to provide adequate protection on client computers. Use the information below as an additional reference to enhance security or achieve better performance. Some of the recommendations provided below are the default settings for the product.

TABLE F-3. Server configuration worksheet

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Manual Scan Settings		
Scan compressed files	Enabled Add compressed files or file extensions you do not want scanned to the scan exclusion list.	
CPU usage	Low This setting helps minimize computer slowdown when scanning occurs during peak hours. To improve performance, consider running Manual Scan during off-peak hours.	
Action	Use ActiveAction	
Real-time Scan Settings		
Real-time Scan	Enabled	
User activity on files	Scan files being created, modified, retrieved, or executed. This option ensures that files introduced to and originating from the computer are safe to access.	

TABLE F-3. Server configuration worksheet (Continued)

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Scan compressed files	Enabled Add compressed files or file extensions you do not want scanned to the scan exclusion list.	
Action	Use ActiveAction	
Display a notification message when a security risk is detected	Enabled Notifications allow users to take immediate action. Consider disabling only if the notifications are generating a large number of support calls.	
Scheduled Scan Settings		
Scheduled Scan	Enabled	
Schedule	Weekly Schedule the scan during off-peak hours to improve the scanning performance and avoid potential computer slowdown.	
Scan target	File types scanned by IntelliScan IntelliScan improves performance by only scanning types known to potentially carry malicious code. Using this setting also allows you to utilize true file-type scanning.	
Scan compressed files	Enabled Add compressed files or file extensions you do not want scanned to the scan exclusion list.	

TABLE F-3. Server configuration worksheet (Continued)

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
CPU usage	Low This setting helps minimize computer slowdown when scanning occurs during peak hours.	
Action	Use ActiveAction	
Allow users to postpone or cancel Scheduled Scan	Disabled Users may cancel the scan if this setting is enabled. Consider enabling only on selected computers. For example, enable the option on a shared computer used for presentations. This allows the user to cancel the scan if scanning will occur during a presentation.	
Scan Exclusion Settings		
Scan exclusions	Enabled Database and encrypted files should generally be excluded from scanning to avoid performance and functionality issues. Also add files that are causing false-positives and files that many users are reporting as safe.	
Web Reputation Settings for External Clients		
Web Reputation policy	Enabled This setting ensures that clients are protected from web-based threats even if they are outside the corporate network.	
Security level	Medium	

TABLE F-3. Server configuration worksheet (Continued)

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Web Reputation Settings for Internal Clients		
Web Reputation policy	Enabled	
Security level	Medium or Low	
Allow clients to send logs to the Trend Micro Security Server	Enabled if you want to monitor websites that users are accessing. This setting generates traffic between the server and clients.	
Web Reputation Approved URL List		
Approved URL list	Add URLs that you or users think are safe to access. Also access the following page if you think a URL has been misclassified: http://reclassify.wrs.trendmicro.com/wrsonlinequery.aspx	
Server Updates		
Update schedule	Daily or Hourly	
Update source	Trend Micro ActiveUpdate server Setting up and maintaining a custom update source may be a tedious process and requires additional computing resources.	

TABLE F-3. Server configuration worksheet (Continued)

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Standard Notifications		
Criteria	Send a notification only when the scan action was not performed successfully Select this option to limit the amount of email notifications you receive and focus only on security events that require your attention.	
Email	Add all Trend Micro Security and Worry-Free Business Security administrators in your organization as email recipients.	
Outbreak Notifications		
Criteria	Use the default settings: • Unique sources: 1 • Detections: 100 • Time period: 24 hours	
Email	Add all Trend Micro Security and Worry-Free Business Security administrators in your organization as email recipients.	
Client-Server Communication		
Server name and listening port	Avoid changing when clients have been registered to the server or clients will have to be redeployed.	

TABLE F-3. Server configuration worksheet (Continued)

CONFIGURATION ITEM	RECOMMENDATIONS	YOUR INFORMATION
Proxy settings	Disabled Clients do not typically communicate with the server through an intranet proxy. Also avoid changing when clients have been registered to the server or clients will have to be redeployed.	
External Proxy Settings		
Proxy settings	Enabled if the Trend Micro Security Server connects to the Trend Micro ActiveUpdate server through a proxy server	
Log Maintenance		
Scheduled deletion of logs	Enabled	
Logs to delete	Logs older than 7 days	
Log deletion schedule	Weekly Schedule the deletion during off-peak hours.	



Migrating from Other Anti-Malware Applications

Migrating from Other Anti-Malware Applications

WFBS 7.0 supports migration from other anti-malware applications.

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

Migrating from antivirus software to WFBS is a two-step process: the installation of the Trend Micro Security Server, followed by the automatic migration of the clients. Automatic client migration refers to replacing existing client antivirus software with the Security Agent program. The client setup program automatically removes the other antivirus software on your client computers and replaces it with the Security Agent. Refer to [Table G-1](#) for a list of client applications that WFBS can automatically remove.

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

TABLE G-1. Removable Antivirus Applications

TREND MICRO™		
Trend Micro Internet Security 2008/2009/2010	Worry-Free Business Security Service 2.5/3.0	
Trend Micro Internet Security Pro 2008/2009/2010	Trend Micro OfficeScan 8.0/10.0/10.5	
Trend Micro Titanium 1.0		
Trend Micro Titanium 2.2/3.0		
SYMANTEC™		

TABLE G-1. Removable Antivirus Applications (Continued)

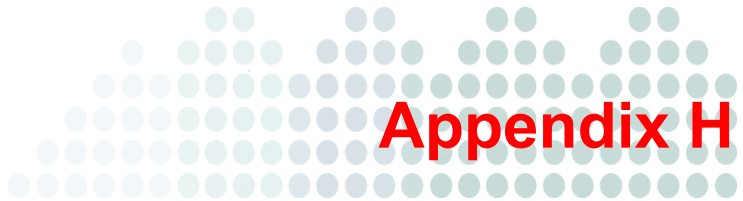
Norton Antivirus CE 8.0 9x	Norton AntiVirus 2008/2009/2010	
Norton Antivirus CE 8.0 NT	Symantec Internet Security 2008/2009/2010	
Norton Antivirus CE 8.1 server	Norton 360 v200	
Norton Antivirus CE 9.0	Symantec Endpoint Protection 11/12	
Norton Antivirus CE 10.0	Symantec AntiVirus 10/11/12	
Norton Antivirus CE 10.1	Symantec Client Security 10/11/12	
McAfee™		
McAfee VirusScan ASaP	McAfee VirusScan Enterprise 7	
McAfee VirusScan ASaP	McAfee VirusScan NT	
McAfee Managed VirusScan	McAfee VirusScan Enterprise 7/8/8.5/8.7	
McAfee SpamKiller	McAfee Anti-Spyware Enterprise 8.0	
McAfee SecurityCenter 7	McAfee Desktop Firewall 8.0	
	McAfee Internet Security 2009	
	McAfee VirusScan Professional 9.0	
LANdesk™		
LANdesk VirusProtect5.0		
COMPUTER ASSOCIATES™		

TABLE G-1. Removable Antivirus Applications (Continued)

CA InocuLAN 5 CA eTrust InoculateIT 6.0/7.0/7.1	CA eTrustITM 8.0/8.1 CA iTechnology iGateway 4.0/4.2	
AHNLAB™		
V3Pro 2000 Deluxe	V3Pro 98 Deluxe	
PANDA SOFTWARE™		
Panda Antivirus Local Networks	Panda Antivirus 6.0	Panda Antivirus Windows NT WS Panda Platinum Internet Security 2004/2005 Panda Platinum 7.0 Panda Titanium Antivirus 2007
F-SECURE™		
F-Secure 4.04 F-Secure 4.08, 4.3 5.3	F-Secure BackWeb F-Secure Client Security 7.10 - E-mail Scanning F-Secure Client Security 7.10 - System Control F-Secure Client Security 7.10 - Internet Shield F-Secure Client Security 7.10 - Web Traffic Scanning	F-Secure Management Agent F-Secure Anti-Virus 2008 F-Secure Internet Security 2008 F-Secure Anti-Virus for Workstations 7.11 F-Secure Anti-Virus for Workstations 8.00
KASPERSKY™		

TABLE G-1. Removable Antivirus Applications (Continued)

Kaspersky Internet Security 2009/2010		
Kaspersky Anti-virus 6.0		
Kaspersky Internet Security 7.0		
MICROSOFT™		
Microsoft Forefront Client Security Antimalware Service 1.0/1.5		
Microsoft Forefront Client Security State Assessment Service 1.0		
Microsoft OneCare 2.x		
SOPHOS™		
Sophos Anti-Virus 9X		
Sophos Anti-Virus NT 5.0/7.0		
Sophos Anti-Virus NT 7.0		
AUTHENTIUM™		
Command AV 4.64 9x		
AMREIN™		
Cheyenne AntiVirus 9X	Cheyenne AntiVirus NT	
GRISOFT™		
Grisoft AVG 6.0/7.0		
AVG Free 8.5/9.0		
OTHERS		
ViRobot 2k Professional	Tegam ViGUARD 9.25e for Windows NT	



Best Practices for Protecting Your Clients

This appendix provides you with some best practices that help you better protect the clients on your network.

Best Practices

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

- Use the Trend Micro recommended WFBS 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 website 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 websites 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 WFBS cannot detect as an Internet threat, send it to Trend Micro:

<http://subwiz.trendmicro.com/SubWiz>

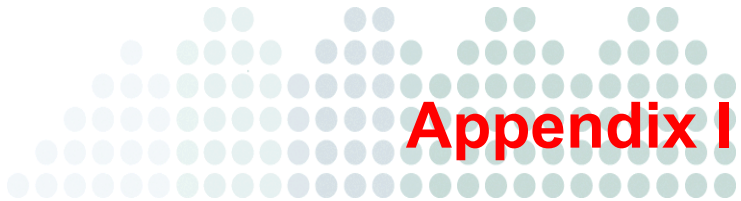
TrendLabs will analyze the files and applications you submit.

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 website and read the *Safe Computing Guide* and other security information.

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



Getting Help

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

The topics discussed in this appendix include:

- *Product Documentation* starting on page I-2
- *Knowledge Base* starting on page I-3
- *Technical Support* starting on page I-3
- *Contacting Trend Micro* starting on page I-4
- *Virus Threat Encyclopedia* starting on page I-6

Product Documentation

The documentation for WFBS consists of the following:

- Online Help

Web-based documentation accessible from the Web Console.

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

Who should use the online help?

WFBS Administrators who need help with a particular screen.

- Installation Guide

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

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

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

Who should read this guide?

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

- Administrator's Guide

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

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

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

Who should read this guide?

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

- Readme file

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

- Knowledge Base

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

<http://esupport.trendmicro.com>

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

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

Knowledge Base

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

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

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

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

Technical Support

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

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

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

To contact Trend Micro Technical Support:

1. Run the Case Diagnostic Tool. For more information, refer *Using the Case Diagnostic Tool* on page I-4.
 - Visit the following URL:
<http://esupport.trendmicro.com/support/srf/questionentry.do>
Click the link for the required region. Follow the instructions for contacting support in your region.
 - If you prefer to communicate by email message, send a query to the following address:
virusresponse@trendmicro.com
 - In the United States, you can also call the following toll-free telephone number:
(877) TRENDAY, or 877-873-6328

Using the Case Diagnostic Tool

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

Download the Case Diagnostic Tool from:

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

Contacting Trend Micro

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

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

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

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

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

Get a list of the worldwide support offices:

<http://www.trendmicro.com/support>

Get the latest Trend Micro product documentation:

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

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

Trend Micro, Inc.

10101 North De Anza Blvd.

Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Web address: www.trendmicro.com

Email: support@trendmicro.com

Sending Suspicious Files to Trend Micro

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

<http://subwiz.trendmicro.com/SubWiz>

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

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

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

Virus Threat Encyclopedia

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

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

Visit the Threat Encyclopedia to:

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

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

TrendLabs

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

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

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

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



Glossary

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

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

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

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

TABLE J-1. Glossary

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

TABLE J-1. Glossary (Continued)

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

TABLE J-1. Glossary (Continued)

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

TABLE J-1. Glossary (Continued)

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

TABLE J-1. Glossary (Continued)

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

TABLE J-1. Glossary (Continued)

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



Trend Micro Product Exclusion List

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

TABLE K-1. Trend Micro Product Exclusion List

PRODUCT NAME	INSTALLATION PATH LOCATION
InterScan eManager 3.5x	HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\InterScan eManager\CurrentVersion ProgramDirectory=
ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange eManager\CurrentVersion ProgramDirectory=
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=

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

PRODUCT NAME	INSTALLATION PATH LOCATION
InterScan Web Security Suite (IWSS)	HKEY_LOCAL_MACHINE\Software\TrendMicro\InterScan Web Security Suite Program Directory= C:\Program Files\Trend Micro\IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion ProgramDirectory={Installation Drive}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion ProgramDirectory=

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

PRODUCT NAME	INSTALLATION PATH LOCATION
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\IM Security\CurrentVersion HomeDir= VSQuarantineDir= VSBBackupDir= FBArchiveDir= FTCFArchiveDir=
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advanc e QuarantineFolder=

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

PRODUCT NAME	INSTALLATION PATH LOCATION
ScanMail for Microsoft Exchange (SMEX) Continued	HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange\QuarantineManager QMDir=

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

PRODUCT NAME	INSTALLATION PATH LOCATION
ScanMail for Microsoft Exchange (SMEX) Continued	Get exclusion.txt file path from HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir Go to HomeDir path (for example, C:\Program Files\Trend Micro\Messaging Security Agent\) Open exclusion.txt C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

Exclusion List for Microsoft Exchange Servers (Advanced only)

By default, when the Security Agent is installed on a Microsoft Exchange server (2000 or later), it will not scan Microsoft Exchange databases, Microsoft Exchange log files, Virtual server folders, or the M drive. The exclusion list is saved in:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\
CurrentVersion\Misc.
```

```
ExcludeExchangeStoreFiles=C:\Program Files\Exchsrvr\mdbdata\
privl.stm|C:\Program Files\Exchsrvr\mdbdata\
privl.edb|C:\Program Files\Exchsrvr\mdbdata\
publ.stm|C:\Program Files\Exchsrvr\mdbdata\publ.edb
```

```
ExcludeExchangeStoreFolders=C:\Program Files\Exchsrvr\mdbdata\
|C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue\
```

```
|C:\Program Files\Exchsrvr\Mailroot\vsi 1\PickUp\  
|C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail\
```

For other Microsoft Exchange recommended folders, please add them to scan exclusion list manually. See:

<http://support.microsoft.com/kb/245822/>

Index

A

- action bar, Data Loss Prevention screen 67, 79
- Activation Code 11, 13, 64
- ActiveAction 4, 50
- ActiveMQ 3, 4, 13
- ActiveUpdate 6
- ActiveUpdate server 33, 35
- Add details section, Data Loss Prevention 69
- Add keyword(s) section, Data Loss Prevention 78
- Add-ins 16
- Administrative Tools 2
- Administrator's Guide 2
- Advanced Macro Scanning 112
- Advanced Options
 - archive directory (Data Loss Prevention) 69
 - section of the Add Rule screen 70
- Adware 12
- adware 41
- Agent
 - Messaging Security Agent overview 3
 - Program 12
 - removing inactive 13
 - Uninstallation 11
- Agent Installation
 - Client Packager 9
 - deployment methods 4
 - Email Notification 16
 - Internal Web Page 5
 - Login Script Setup 6
 - Management Console 16
 - MSI File 11
 - overview 3
 - verifying 17
 - Vulnerability Scanner 14, 18
 - Windows Remote Install 12
- Alerts
 - email notifications for events 6
 - firewall violation on client 8
 - global settings 11
 - status alerts for Outbreak Defense 5
- Allowing Programs 19
- Anti-Spam
 - components 7
 - content scanning 30
 - managing spam 105
 - POP3 mail scan 17
 - reports 9
 - Spam Detection Level 38
 - Spam Mail folder 102
 - viewing threat status 9
- Anti-Spyware
 - components 6
 - reports 9
 - viewing threat status 9
- Antivirus
 - components 6
 - reports 8
 - viewing threat status 8
- Apple Remote Desktop 22, 26
- Approved Email Senders 38
- Approved List for Spyware/Grayware 14
- Approved List of Programs 19
- approved list, Data Loss Prevention 83
- Approved Senders section, Data Loss Prevention 83
- Approved Senders section, Data Loss Prevention screen 83
- archive 69
 - Data Loss Prevention action 69
 - directory 69
- archive directory
 - default (Data Loss Prevention) 70
 - field, Data Loss Prevention 70
- Archive Email Messages 6

- Archive Setting subsection, Advanced Options section, Add Rule screen (Data Loss Prevention) 70
- Archive Utility 23, 26
- Attachment Blocking 87
 - settings 89
- Attachment field, selecting as target 69
- autopcc.exe 7, 8
- Autorun Files 17

B

- Backdoor Programs 11
- bank account numbers 65
- Behavior Monitoring 17
 - components 9
 - protection from USB threats 17
 - reports 10
 - viewing threat status 9
- Benefits of Protection 5
- Best Practices 2
- Blocked
 - Email Senders 38
 - Programs List 19
- Blocking
 - Programs 19
 - Unwanted Web Content 16
 - Web Threats 15
- Body field, selecting as target 69
- boot sector virus 39
- Bots 12
- Browser Cache 6
- business information, confidential 65

C

- Case Diagnostic Tool 4
- Cc field, selecting, Data Loss Prevention 69
- clean files 49
- Client
 - 32-bit and 64-bit 8
 - adding to a group 5
 - importing and exporting settings 6
 - Location Awareness 8
 - moving between groups 5
 - privileges 23
 - protection from USB Threats 17
 - removing from Management Console 7
- client icons 67
- client installation 22
 - post-installation 29
 - problems 71
 - requirements 21

- Client Mover 14
- Client Packager 9, 11
 - using the graphical user interface 9
- Client Tools 11
- client tree 17
 - general tasks 18
- client uninstallation 31
- client update 30, 37
- client upgrade 60
- client-server communication 65
- Compatibility 12
- Components
 - anti-spam 7
 - anti-spyware 6
 - antivirus 6
 - Behavior Monitoring 9
 - Content Filtering 9
 - network viruses 8
 - Outbreak Defense 8
 - software protection 9
 - that can be updated 18
 - Transaction Protector 9
 - TrendProtect 9
 - updating 18
 - updating with ActiveUpdate 4
 - Web Reputation 8
- components 17, 32
 - on the client 37
 - on the server 34
- compressed file scanning 46
- Compressed Files
 - scanning 8
- Computers 11
- confidential business information 65
- Configure Settings 13
- Conflicting ARP 12
- Connection
 - Client and Server 14
- Contacting Trend Micro 4
- Content Filtering 39
 - adding rules 41
 - components 9
 - global settings for messenger programs 10
 - regular expressions 55
 - reordering rules 65
 - reports 10
 - using keywords 49
 - viewing rules 63

Content Scanning 30

settings 37

Conventional Scan 3

D

Damage Cleanup Services 2

Data Loss Prevention 65, 69

Add keyword(s) section 78

approved list 83

Approved Senders section 83

archive

action 69

directory 69

Archive directory field 70

Archive Setting subsection, Advanced Options, Add Rule screen 70

default rules 68

delete entire message 69

deleting rules 78

Do not notify external recipients (senders) option 70

domain accounts, excluding from filtering 82

domain, does not add until you click "Save" 83

Edit Rule screen 77

editing rules 77

email

account, adding a specific account to exclude from 83

addresses, importing a list for exclusion from 84

enable or disable a rule 80

Enable this rule check box 81

export

approved senders (whole list only) 85

list of email accounts 85

rules 78

rules, multiple select 78, 79

Export action button 79

icons, rules, disabled and enabled 81

Import action button 79

importing

rules 78

rules from a plain-text file 79

keyword rules 69

kinds of rules 67

manually entering regular expression 76

Notification section 70

page-navigation icons 77

preparatory work 66

quarantine

entire message 69

message part 69

Quarantine directory field 70

regular expression

(Auto-generate) option 73

(User-defined) option 72, 76

auto-generator tool, testing a generated expression 75

manually entering 76

prefix when manually entered 76

used in default rules, by region 68

reordering rules 85

Replace with text/file 69

Replacement file name field 70

Replacement Settings subsection, Advanced Options, Add Rule screen 70

Replacement text field 71

rule action 69

Rule Name field is required 76

rule notification 69

rules

disabling 80

editing 77

enabling 80

removing 78

rules list, enabling rules from 80

Select target section 69

Specific Domain Account(s) excluded from Data Loss Prevention 82

target selection 69

undelete, there is no undelete for removing rules 78

Data Loss Prevention screen, Rules section 67

Data Loss Prevention, enabling 66

Debugger 106

default

archive directory, Data Loss Prevention 70

quarantine directory, Data Loss Prevention 70

replacement file name, Data Loss Prevention 70

replacement text, Data Loss Prevention 71

default rules, Data Loss Prevention 68

Default Settings 3

Delete entire message 69

Device Control 20

dialer 41

Dialers 12

DLP. See Data Loss Prevention.

Do not notify external recipients (senders), Data Loss Prevention 70

- Documentation 2
- domain accounts, excluding from filtering, Data Loss Prevention 82
- Downloading
 - program updates 3

E

- Edit Rule screen, Data Loss Prevention 77, 81
- Edit Rule screen, Data Loss Prevention, enabling or disabling a rule from 80
- editing a rule 77
- EICAR Test Virus 20
- email
 - approved list, Data Loss Prevention 83
 - exporting list of approved accounts, Data Loss Prevention 85
- email account, adding a specific account to exclude from, Data Loss Prevention 83
- email addresses, importing a list for exclusion from Data Loss Prevention 84
- Email Messages
 - adding a disclaimer 108
 - adding a header tag 6
 - approved senders 38
 - archiving 6
 - blocked senders 38
 - blocking attachments 87
 - cleaning threats 5
 - content filtering 39
 - content scanning 30
 - deleting threats 6
 - quarantine 6
 - quarantine entire message 5
 - quarantine to client spam folder 6
 - quarantine to server 6
 - wildcard matching 35
- Email Notification to Install Agent 16
- Email Reputation 4, 29, 7
- enable or disable a rule, Data Loss Prevention 80
- Enable this rule check box
 - Data Loss Prevention 81
 - must click Save to enable (Data Loss Prevention) 82
- enabling Data Loss Prevention 66
- End User Quarantine Tool 101
- Environment Variables 20

- Exceptions
 - Behavior Monitoring 19
 - firewall 8, 9
 - Outbreak Defense 14
 - using environment variables 20
- Exclusions
 - Trend Micro products not scanned 1
- export
 - approved senders list, can export only the whole list, Data Loss Prevention 85
 - list of email accounts, Data Loss Prevention 85
- Export action button, Data Loss Prevention 79
- Export Settings 6
- exporting rules
 - can select rules that appear on one screen only 79
 - Data Loss Prevention 78
 - from multiple screens 79
 - multiple select, Data Loss Prevention 78, 79
 - plain-text file format 78
- external mail recipients, turn off notification of (Data Loss Prevention) 70

F

- Fake Access Points 13
- Features 2
- Features of Product 3
- fields, required (Data Loss Prevention) 73
- File Reputation 4
- Filtering
 - spam from known spammers 4
- Firewall 4
 - default settings 5
 - enable or disable 8
 - exceptions 8, 9
 - Intrusion Detection System 11
 - mode 8
 - network viruses 6
 - security level 8
 - settings 8
 - stateful inspection 6
 - traffic filtering 6
- firewall 65
- Fragmented IGMP 12
- From field, selecting (Data Loss Prevention) 69

G

- Getting Help 6
- Global Settings 1
 - agent uninstall 11
 - agent unload 12
 - alerts 11
 - desktops and servers 6
 - general scan settings 8
 - Help Desk Notice 7
 - Location Awareness 7
 - messaging content filtering 10
 - proxy server 3
 - quarantine folder 15
 - SMTP server 5
 - Spyware/Grayware settings 9
 - URL Filtering 9
 - virus scan settings 8
 - Watchdog settings 11
 - Web Reputation 10
- Groups 2
 - adding 4
 - adding clients 5
 - moving clients 5
 - removing clients 7
 - replicating settings 6
- groups 17, 20

H

- Hacking Tools 12
- hacking tools 41
- Header email field, Data Loss Prevention 69
- Help Files 2
- Help Icon 6
- Hot Fixes 3

I

- Icons
 - Live Status screen 8
 - Web Console 6
- icons, rules, disabled and enabled, Data Loss Prevention 81
- ICQ Instant Messenger 10
- Import action button, Data Loss Prevention 79
- Import File window
 - Data Loss Prevention 80
- import format for rules 79
- Import Settings 6
- importing
 - email list for exclusion 84
 - rules, Data Loss Prevention 78, 79

- Inactive Agents 13
- information, confidential business 65
- installation
 - client 22
 - server 9
- Installation Guide 2
- installation package 22
 - corruption 23, 26
- Installing Agents 2
 - Client Packager 9
 - Email Notification 16
 - Internal Web Page 5
 - Login Script Setup 6
 - Management Console 16
 - MSI File 11
 - verifying 17
 - Vulnerability Scanner 14, 18
 - Windows Remote Install 12
- Instant Messenger
 - content filtering 10
 - threats 13
- IntelliScan 4
- IntelliTrap 6
- Internal Web Page 5
- Intrusion Detection System 11
- Intuit Software 13
- Itanium 2 Architecture 8

J

- joke program 39
- JRE 4, 15

K

- Keyloggers 12
- keyword rule, character limitations, Data Loss Prevention 69
- keyword, adding rules by, Data Loss Prevention 69
- Keywords 49
- kinds of rules, Data Loss Prevention 67
- Knowledge Base 2, 3

L

- LAND Attack 12
- Language
 - changing 6
- Leopard operating system 21

- License
 - changing 4
 - event notifications 3
 - expiration 4
 - renewing 4
 - viewing 3
 - viewing license status 10
- license 64
- license agreement 11
- Live Status 10
 - icons 8
 - license status 10
 - overview of screen 7
 - system status 9
 - threat status 8
 - update intervals 10
- Location Awareness 7, 8
- Login Script Setup 6, 3
- Logs 2
 - automatically deleting 6
 - console events 2
 - deleting 6
 - desktop/server 3
 - manually deleting 7
 - Messaging Security Agents 4
 - querying 4
- logs
 - maintenance 63
 - security risks 54
 - Web threats 59

M

- Mac OS X 21
- Macintosh 2, 22, 26, 31
- macro virus 39
- Macro Viruses 11
- mail recipients, external 70
- Main Menu 4
- Malicious Behavior 13
- Malware 10
- malware 38
- Management Console 2
 - Agent Installation 16
 - password 2
- Management console
 - unable to access 69
- Manual Scan 3, 43
 - shortcut on Windows menu 9
- Mass-Mailing Attacks 14
- MDAC 4

- message without content, quarantine message part 69
- Messaging Security Agent 3
 - actions 5
 - antivirus options 12
 - Debugger 106
 - default settings 7
 - Email Reputation 29
 - logs 4
 - monitoring in real-time 90
 - notification settings 7
 - notifications 103
 - quarantine 93
 - replicating settings 108
 - scan options 7
 - scanning 4
- Microsoft Exchange Servers
 - folders not scanned 5
- Microsoft Visual C++ 4
- Mixed Threat Attack 11
- MSA 3
- MSI File 11
- MSN Messenger 10

N

- Network Virus 12, 6
 - components 8
 - logs 3
 - reports 10
 - viewing threat status 9
- New Features 2
- Notification section, Data Loss Prevention 70
- notification, of Data Loss Prevention action 69
- Notifications 10, 2
 - event settings 3
 - for license events 3
 - for system types 3
 - for threats 2
 - MSA 103
 - notifications 50, 51
 - outbreak 52
 - security risks 51
- Notify recipients, Data Loss Prevention 70
- Notify senders, Data Loss Prevention 70

O

- OLE Layers 8
- Online Keystroke Listeners 13
- Outbreak Defense
 - actions 4
 - components 8
 - exceptions 14
 - logs 3
 - potential threat 8
 - recommended settings 12
 - red alerts 2
 - reports 9
 - settings 10
 - status alerts 5
 - strategy 2
 - threat cleanup 6
 - threat information 5
 - threat prevention 5
 - threat protection 6
 - viewing current status 4
 - viewing threat status 9
 - vulnerable computers 5, 9
 - yellow alerts 2
- Outbreak Prevention Policy 2
- outbreaks 52
- Overlapping Fragment 12
- Oversized Fragment 11
- Overview of Product 2

P

- packer 40
- Packers 13
- page-navigation icons 80, 81
- page-navigation icons, Data Loss Prevention 77
- Password 13
 - changing for Management Console 2
- password cracking applications 41
- Patches 3
- Phishing 13, 31
- phishing 32
- Ping of Death 12
- Plug-in Manager 3
- POP3 Mail Scan 17
- Ports
 - Outbreak Defense exceptions 12
- post installation
 - client 29
 - server 13
- Privileges
 - for clients 23

- probable virus/malware 40
- Product
 - documentation 2
 - features 3
 - overview 2
- programs 17, 32
- Protecting Your Network 2
- Proxy Server
 - settings 3
- proxy settings
 - client update 65
 - server update 35

Q

- Quarantine
 - delete all files 16
 - directory settings 26
 - directory settings for MSA 94
 - email messages in client spam folder 6
 - End User Quarantine tool 101
 - entire email messages 5
 - folder capacity 16
 - global settings 15
 - management 25
 - maximum size for a file 16
 - MSA folder 93
 - parts of email messages 6
 - querying MSA directories 97
- quarantine 69, 49, 55
- quarantine directory
 - Data Loss Prevention 69
 - default, Data Loss Prevention 70
- Quarantine directory field, Data Loss Prevention 70
- Quarantine entire message, with Data Loss Prevention 69
- quarantine message part, Data Loss Prevention 69
- QuickBooks 19

R

- Readme file 2
- Real-time Monitor 90
- Real-time Scan 2, 42
- recipients, external mail 70
- red alerts 2
- Registration 12
- Registration Key 11
- Regular Expression (Auto-generate) option, Data Loss Prevention 73, 78
- Regular Expression (User-defined) option, Data Loss Prevention 72, 76, 78

- Regular Expression field
 - type, do not paste 76
 - regular expression generator, limitations 71
 - Regular Expressions 55
 - regular expressions
 - .REG. prefix 76
 - auto-generator 72
 - auto-generator example field 73
 - auto-generator tool limitations 75
 - auto-generator tool, shaded area 73
 - auto-generator tool, verifying using additional examples 75
 - constants, using auto-generator tool 74
 - limitation of test term is 40 characters 77
 - limitations when using auto-generator 71
 - manually entering, Data Loss Prevention 76
 - pasting is not advised 76
 - prefix 76
 - testing manually entered 76
 - things to consider when using with Data Loss Prevention 71
 - used in default rules based on region, Data Loss Prevention 68
 - using auto-generator tool 72
 - verifying 77
 - remote access tools 41
 - Removing Agents 20
 - Replace with text/file
 - Data Loss Prevention action 69
 - fields can apply to 69
 - Replacement file name field, Data Loss Prevention 70
 - Replacement Settings subsection, Data Loss Prevention 70
 - Replacement text field, Data Loss Prevention 71
 - Replicating Settings 6
 - Reports 7
 - anti-spam 9
 - anti-spyware 9
 - antivirus 8
 - Behavior Monitoring 10
 - Content Filtering 10
 - generating 11
 - interpreting 8
 - managing 14
 - network virus 10
 - Outbreak Defense 9
 - settings 11
 - URL Filtering 9
 - Web Reputation 9
 - required fields
 - Rule Name, Add Keyword, Data Loss Prevention 73
 - Rule Name, Data Loss Prevention 76
 - restart services 66, 71
 - Restore Encrypted Virus 12
 - Rootkits 11
 - rule action 69
 - Rule Name field 76
 - rules
 - creating 69
 - deleting, Data Loss Prevention 78
 - disabling, Data Loss Prevention 80
 - editing 77
 - enabling from the rules list 80
 - icons, disabled and enabled 81
 - keyword 69
 - kinds of Data Loss Prevention 67
 - locating an edited rule in the rules list 77
 - rules enabling, Data Loss Prevention 80
 - rules list
 - enabling rules from, Data Loss Prevention 80
 - locating an edited rule in 77
 - locating edited rule in 77
 - Rules section, Data Loss Prevention screen 67
- ## S
- Safe Computing Guide 3
 - SBS and EBS Add-ins 17
 - scan actions 48
 - scan criteria 45
 - CPU usage 47
 - scan compressed files 46
 - scan target 46
 - schedule 47
 - user activity on files 45
 - scan exclusions 48
 - Scan Methods 3
 - Scan Now 30, 45
 - scan results 55
 - Scan Server
 - definition 15
 - Scan Types 2
 - scan types 42
 - Manual Scan 43
 - Real-time Scan 42
 - Scan Now 45
 - Scheduled Scan 44

- Scanning
 - adding Manual Scan shortcut 9
 - Advanced Macro Scanning 112
 - by schedule 3, 9
 - compressed files 8
 - Conventional Scan 3
 - Exchange Server folders not scanned 5
 - general scan settings 8
 - logs 3
 - manual (on demand) 3
 - Messaging Security Agent options 12
 - Messaging Security Agents 7
 - MSA email scans 4
 - OLE layers 8
 - POP3 mail 17
 - Real-time 2
 - Smart Scan 5, 3
 - Trend Micro products not scanned 1
 - Scheduled Scan 3, 9, 44
 - postpone or cancel 50
 - Security Agent Program Exit Password 12
 - Security Agent Uninstallation Password 11
 - Security Information Center 73
 - security risks 38
 - logs 54
 - outbreak 52
 - phish attacks 32
 - spyware and grayware 40
 - viruses and malware 38
 - security summary 16
 - components and programs 17
 - networked computers 16
 - Select an action section, Data Loss Prevention 69
 - Select target section, Data Loss Prevention 69
 - Sending Possible Threats to Trend Micro 3
 - server installation 9
 - post-installation 13
 - requirements 4
 - update source 9
 - server name/IP address 66
 - server uninstallation 15
 - problems 71
 - server update 34
 - manual update 37
 - proxy settings 35
 - update methods 36
 - server upgrade 60
 - Service Packs 3
 - Settings
 - virus scan settings 8
 - Smart Feedback 3, 5
 - Smart Protection Network 3, 5
 - Smart Scan 5, 3
 - viewing system status 10
 - SMTP Server 5
 - social security numbers 65
 - Software Protection
 - components 9
 - Spam 12, 30
 - blocking known spammers 4
 - managing 105
 - Spam Detection Level 38
 - Spam Mail Folder 102
 - Specific Domain Account(s) excluded from Data Loss Prevention section 82
 - spyware 41
 - Spyware Active-monitoring Pattern 32
 - Spyware/Grayware
 - approved list 14
 - global settings 9
 - SQL server 4, 13
 - SSL certificate 7
 - SSN. See social security number.
 - Stateful Inspection 6
 - Subject field, selecting, Data Loss Prevention 69
 - summary
 - security 16
 - Support 3
 - SYN flood 12
 - System Event Notifications 3
 - system tray icons 67
- ## T
- Target tab, “Select target” section 77
 - Target, selecting for Data Loss Prevention 69
 - Teardrop Attack 12
 - Technical Support 3
 - telephone numbers 65
 - Terminal utility 72
 - test regular expressions
 - auto-generator tool, Data Loss Prevention 75
 - manually entered regular expression 76
 - Test Virus 20
 - test virus 40
 - text file, importing, Data Loss Prevention 84
 - Threat Notifications 2

- Threats 10
 - adware 12
 - backdoor programs 11
 - bots 12
 - Conflicting ARP 12
 - dialers 12
 - fake access points 13
 - Fragmented IGMP 12
 - hacking tools 12
 - in messenger programs 13
 - intrusions 13
 - keyloggers 12
 - LAND Attack 12
 - macro viruses 11
 - malicious behavior 13
 - malware 10
 - mass-mailing attacks 14
 - Mixed Threat Attack 11
 - network viruses 12
 - online keystroke listeners 13
 - Overlapping Fragment 12
 - Oversized Fragment 11
 - packers 13
 - Phishing 31
 - phishing 13
 - Ping of Death 12
 - rootkits 11
 - spam 12
 - spyware 11
 - SYN flood 12
 - Teardrop Attack 12
 - Tiny Fragment Attack 12
 - Trojans 10
 - viruses 10
 - Web threats 4
 - worms 11
 - Tiger operating system 21
 - Tiny Fragment Attack 12
 - TMVS.ini 7
 - To field, selecting, Data Loss Prevention 69
 - token variable 52, 53
 - Tools 2
 - Client Mover 14
 - Client Packager 11
 - Login Script Setup 3
 - Restore Encrypted Virus 12
 - Vulnerability Scanner 3
 - Traffic Filtering 6
 - Transaction Protector
 - components 9
 - Transport Neutral Encapsulation Format 14
 - Trend Micro contact URL 4
 - Trend Micro Security
 - about 2
 - client 3
 - components 17, 32
 - programs 17
 - server 2
 - web console 15
 - Trend Micro Security client 3
 - Trend Micro Security server 2
 - Trend Micro Services
 - Damage Cleanup Services 2
 - Outbreak Prevention Policy 2
 - Vulnerability Assessment 3
 - TrendLabs 7
 - definition 6
 - TrendProtect
 - components 9
 - Trojan horse program 39
 - Trojans 10
 - Troubleshooting 2
 - Activation Code and Registration Key 11
 - client icons 8
 - Client Packager 2
 - clients on Management Console 8
 - components 6
 - program settings 4
 - resending a quarantined message 3
 - spam folder 3
 - Web Console 6
 - troubleshooting 69
 - True File Type 6
- ## U
- UNC paths 19
 - undelete, there is no undelete for removing rules, Data Loss Prevention 78
 - Uninstall
 - Security Server 6
 - Uninstall Agents 20
 - uninstallation
 - client 31
 - server 15
 - uninstallation package 22, 31
 - Uninstalling Agents
 - settings 11
 - with the agent program 21
 - with the Management Console 21
 - Uninstalling Messaging Agents 22

- Unloading Agent
 - settings 12
- Unusual System Events
 - viewing system status 9
- Update Agent 13
- update methods
 - client 37
 - server 36
- update source
 - client 30, 37
 - Plug-in Manager 9
 - server 35
- Updates
 - Outbreak Defense 12
 - viewing system status 9
- updates
 - client 30, 37
 - server 34
- Updating
 - ActiveUpdate 4
 - components 18
 - hot fixes, patches, and service packs 3
 - logs for 3
 - selecting an update source 5
 - settings 2
 - sources 5
 - using ActiveUpdate 6
 - using an update agent 13
- upgrade server and client 60
- URL Filtering 5
 - global settings 9
 - logs 3
 - reports 9
 - settings 16
 - viewing threat status 9
- USB Devices
 - threats 17
- User Tools 22
 - settings 22
- V**
- Variables 20
- Verify
 - client and server connection 14
- Virtual Directory Settings 7
- virus 38
- Virus Logs 3
- Virus Pattern 32
- Virus Scan Engine 32
 - updating 33
- Virus Threat Encyclopedia 6
- VSAPI.dll 12
- VSEncode.exe 12
- Vulnerability Assessment 16, 3
- Vulnerability Scanner 14, 18, 3
 - settings 4
- Vulnerable Computers 5, 9
 - Vulnerability Assessment settings 16
- W**
- Watchdog 11
- Web Console
 - event logs 2
 - icons 6
 - language 6
 - opening 4
 - URL 4
- web console 15
 - requirements 15
 - URL 16
- Web Reputation 4, 10, 8
 - components 8
 - filter strength 16
 - logs 3
 - reports 9
 - scores 8
 - security level 15
 - viewing threat status 9
- Web reputation 57
 - policies 57
- Web Threats 4
 - using Web Reputation 15
- Web threats
 - about 57
 - logs 59
- What's New 2
- whitelist. See Approved Senders and domain accounts, excluding from filtering, Data Loss Prevention
- Wildcards, Content Scanning
 - using wildcards 35
- Windows Essential Business Server 16
- Windows Messenger Live 10
- Windows Remote Install 12
 - on Windows Vista 13
- Windows Shortcut Menu
 - adding Manual Scan 9
- Windows Small Business Server 16
- worm 39
- Worms 11

Y

Yahoo! Messenger 10

yellow alerts 2