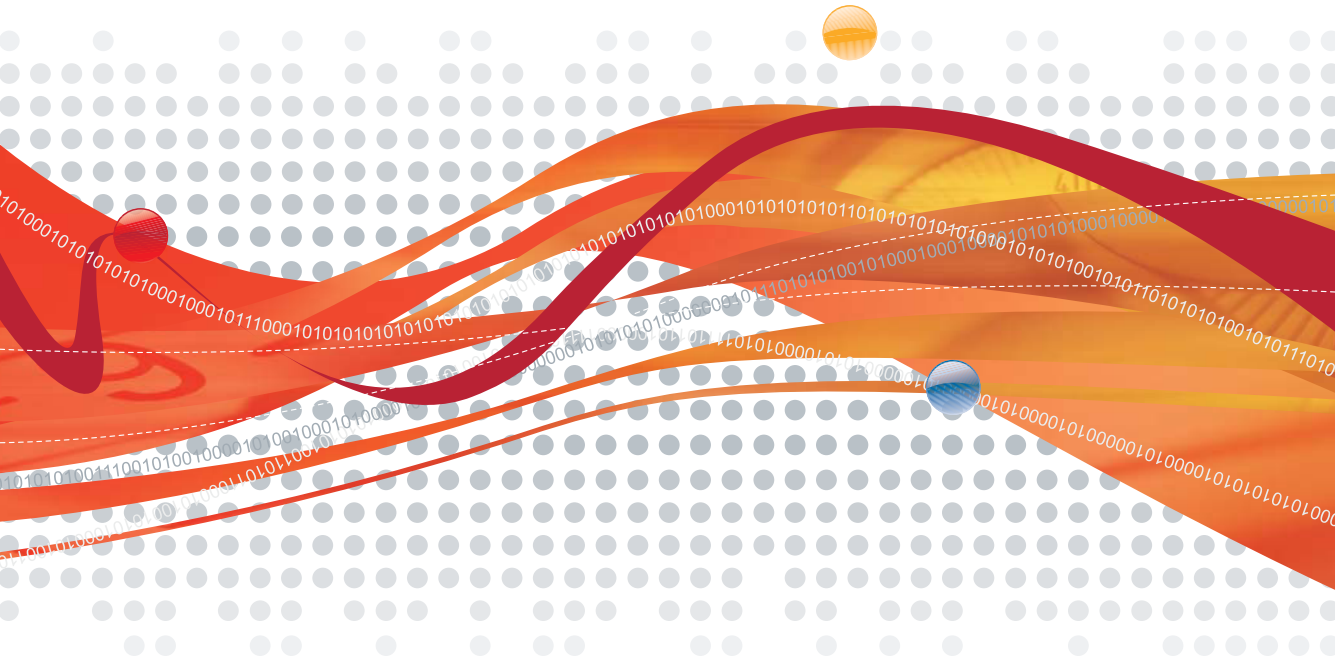
TREND MICRO™

Worry-Free™ Business Security Advanced5

for Small and Medium Business



Administrator's Guide

Release Date: February 2009

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

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

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

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

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

Contents

Preface

Audience xiv
Product Documentation xiv
What Information Can I Find in the Administrator's Guide? xvi
Document Conventions and Terms xvii

Chapter 1: Introducing Worry-Free Business Security Advanced

Overview of Worry-Free Business Security Advanced 1-2
What's New in This Release? 1-2
What's New in Version 5.1 1-2
What's New in Version 5.0 1-4
What's Included in Worry-Free Business Security Advanced 1-5
Web Console 1-7
Security Server 1-7
Client/Server Security Agent 1-8
Messaging Security Agent 1-9
Scan Engine 1-9
Virus Pattern File 1-10
Virus Cleanup Engine 1-11
Common Firewall Driver 1-12
Network Virus Pattern File 1-12
Vulnerability Pattern File 1-12
Understanding Threats 1-12
Virus/Malware 1-12
Spyware/Grayware 1-13
Network Viruses 1-14
Spam 1-15
Intrusions 1-15
Malicious Behavior 1-15
Fake Access Points 1-15
Explicit/Restricted Content in IM Applications 1-15
Online Keystroke Listeners 1-15
Packers 1-16

Phishing Incidents 1-16
Mass-Mailing Attacks 1-16
How Worry-Free Business Security Advanced Protects Your Computers and Network 1-17
About Components 1-17
Other Supplementary Trend Micro Products 1-21
What Else Can Worry-Free Business Security Advanced Do? 1-21
Manage Security From a Single Console 1-22
Analyze Network Protection 1-22
Enforce Security Policies 1-22
Have Updated Protection 1-23
Quarantine Infected Files 1-23
Control Outbreaks on the Network 1-23
Manage Worry-Free Business Security Advanced Groups 1-23
Protect Clients from Hacker Attacks with Firewall 1-24
Protect Email Messages 1-24
Filter Instant Messaging Content 1-24
Control Security Settings Based on Location 1-24
Behavior Monitoring 1-25
Protect Clients from Visiting Malicious Web Sites 1-26
Facilitate Safe Online Transactions 1-27
Approved Spyware/Grayware Programs 1-27
Secure Communication 1-28
Updateable Components 1-28
Hot Fixes, Patches, and Service Packs 1-28

Chapter 2: Working With the Web Console

Exploring the Web Console 2-2
Web Console Features 2-4
Using Live Status and Notifications 2-6
Setting Up Notifications 2-6
Using Live Status 2-7
Threat Status 2-9
System Status 2-14

Chapter 3: Installing Agents

Choosing an Installation Method 3-2
Installing, Upgrading, or Migrating Client/Server Security Agents 3-3
Agent System Requirements 3-4
Performing a Fresh Install 3-5
Installing from an Internal Web Page 3-6
Installing with Login Script Setup 3-7
Installing with Windows 2000/Server 2003/Server 2008 Scripts 3-8
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 MSA from the Web Console 3-16
Verifying the Agent Installation, Upgrade, or Migration 3-17
Using Vulnerability Scanner to Verify the Client Installation 3-17
Testing the Client Installation with the EICAR Test Script 3-19
Removing Agents 3-21
Removing Client/Server Security Agent Using Its Uninstallation Program 3-21
Removing the Client/Server Security Agent using the Web Console 3-21
Removing Messaging Security Agent from Microsoft Exchange Servers 3-22
Removing the Messaging Security Agent using its Uninstallation Program 3-23

Chapter 4: Working with Groups

Overview of Groups 4-2
Viewing Clients in a Group 4-2

Security Settings Toolbar 4-5
Adding Groups 4-6
Removing Groups 4-7
Adding Clients to Groups 4-7
Moving Clients 4-9
Replicating Group Settings 4-10

Chapter 5: Configuring Desktop and Server Groups

Overview of Configurable Options for Desktop and Server Groups 5-2
Antivirus/Anti-spyware 5-3
Configuring Real-time Scan 5-5
Firewall 5-8
Configuring the Firewall 5-11
Web Threat Protection 5-15
Configuring Web Threat Protection 5-15
Behavior Monitoring 5-16
Environment Variables 5-18
Configuring Behavior Monitoring 5-18
TrendSecure 5-21
Configuring TrendSecure 5-21
POP3 Mail Scan 5-23
POP3 Mail Scan Requirements 5-23
Anti-Spam Toolbar Requirements 5-23
Enabling Mail Scan 5-24
Configuring POP3 Mail Scan to Scan Other Ports 5-24
Client Privileges 5-25
Configuring Client Privileges 5-26
Quarantine 5-28
Configuring the Quarantine Directory 5-29

Chapter 6: Configuring Microsoft Exchange Servers

About Messaging Security Agents 6-2
Configurable Options for Microsoft Exchange Server Groups 6-5
Default Messaging Security Agent Settings 6-6
Antivirus 6-7

Configuring Real-time Scan for Messaging Security Agents 6-8
Anti-Spam 6-12
Email Reputation 6-12
Content Scanning 6-13
Configuring Email Reputation 6-17
Content Scanning 6-18
Content Filtering 6-20
Keywords 6-21
Regular Expressions 6-24
Viewing Content Filtering Rules 6-32
Adding/Editing Content Filtering Rules 6-33
Reordering Rules 6-35
Attachment Blocking 6-35
Configuring Attachment Blocking 6-38
Quarantine 6-40
Quarantine Directories 6-41
Configuring Quarantine Directories 6-41
Querying Quarantine Directories 6-43
Maintaining Quarantine Directories 6-46
Managing the End User Quarantine Tool 6-47
Setting up the Spam Folder 6-48
Operations 6-49
Notification Settings 6-50
Spam Maintenance 6-51
Trend Support/Debugger 6-53

Chapter 7: Using Outbreak Defense

Outbreak Defense Strategy 7-2
Outbreak Defense Actions 7-2
Current Status 7-3
Threat Prevention 7-5
Threat Protection 7-7
Threat Cleanup 7-7
Potential Threat 7-9
Setting up Outbreak Defense 7-11
Outbreak Defense Settings 7-12

Configuring Vulnerability Assessment Settings 7-16

Chapter 8: Configuring Manual and Scheduled Scans

Worry-Free Business Security Advanced Scans 8-2
Manual Scan 8-2
Scheduled Scan 8-2
Real-time Scan 8-2
Scanning Clients 8-3
Configuring Scan Options for Groups 8-3
Configuring Scan Options for Microsoft Exchange Servers 8-8
Scheduling Scans 8-12

Chapter 9: Updating Components

Updating Components 9-2
About ActiveUpdate 9-3
Updatable Components 9-3
Default Update Times 9-5
Updating the Security Server 9-6
Update Sources 9-6
Configuring an Update Source 9-8
Using Update Agents 9-9
Manual and Scheduled Updates 9-11
Manually Updating Components 9-12
Scheduling Component Updates 9-13
Rolling Back or Synchronizing Components 9-14

Chapter 10: Viewing and Interpreting Logs and Reports

Logs 10-2
Reports 10-3
Interpreting Reports 10-4
Using Log Query 10-5
Generating Reports 10-7
Managing Logs and Reports 10-10
Maintaining Reports 10-10
Automatically Deleting Logs 10-11
Manually Deleting Logs 10-12

Chapter 11: Working with Notifications

About Notifications 11-2
Threat Events 11-2
System Events 11-3
Configuring Notifications 11-3
Customizing Notification Alerts 11-5
Configuring Notification Settings 11-6

Chapter 12: Configuring Global Settings

Internet Proxy Options 12-2
SMTP Server Options 12-3
Desktop/Server Options 12-3
Location Awareness 12-5
General Scan Settings 12-5
Virus Scan Settings 12-6
Spyware/Grayware Scan Settings 12-7
Web Threat Protection 12-7
Behavior Monitoring 12-7
IM Content Filtering 12-8
Alert Settings 12-8
Watchdog Settings 12-9
Agent Uninstallation 12-9
Agent Unloading 12-9
System Options 12-10
Removing Inactive Client/Server Security Agents 12-11
Verifying Client-Server Connectivity 12-12
Maintaining the Quarantine Folder 12-12

Chapter 13: Performing Additional Administrative Tasks

Changing the Web Console Password 13-2
Working with the Plug-in Manager 13-3
Viewing Product License Details 13-3
Consequences of an Expired License 13-4
Changing your License 13-4
Participating in the Smart Protection Network 13-5
Changing the Agent's Interface Language 13-5
Uninstalling the Trend Micro Security Server 13-6

Chapter 14: Using Administrative and Client Tools

Tool Types 14-2
Administrative Tools 14-3
Login Script Setup 14-3
Vulnerability Scanner 14-3
Client Tools 14-8
Client Packager 14-8
Restore Encrypted Virus 14-8
Touch Tool 14-10
Client Mover 14-11
Add-ins 14-13
Installing the SBS and EBS Add-ins 14-13
Using the SBS and EBS Add-ins 14-14

Chapter 15: FAQs, Troubleshooting, and Technical Support

Frequently Asked Questions (FAQs) 15-2
How can I further protect Clients? 15-2
Registration 15-3
Installation, Upgrade, and Compatibility 15-3
Intuit Software Protection 15-4
Configuring Settings 15-5
Documentation 15-6
Troubleshooting 15-7
Environments with Restricted Connections 15-7
User's Spam Folder not Created 15-7
Internal Sender/Recipient Confusion 15-8
Re-sending a Quarantine Message Fails 15-8
Replicating Settings Fails 15-9
Saving and Restoring Program Settings for Rollback or Reinstallation 15-10
Some Components are not Installed 15-12
Unable to Access the Web Console 15-12
Incorrect Number of Clients on the Web Console 15-13
Unsuccessful Web Page or Remote Installation 15-14
Client Icon Does Not Appear on Web Console after Installation 15-15
Issues During Migration from Other Antivirus Software 15-16

Invalid/Expired Digital Signatures 15-17
Trend Micro Security Information Center 15-18
Known Issues 15-19
Contacting Trend Micro 15-19
Trend Micro Support 15-19
Knowledge Base 15-20
Contacting Technical Support 15-20
Sending Suspicious Files to Trend Micro 15-21
About TrendLabs 15-22
About Trend Micro 15-22

Appendix A: System Checklists

Ports Checklist A-1
Server Address Checklist A-2

Appendix B: Trend Micro Product Exclusion List

Exclusion List for Microsoft Exchange Servers B-3

Appendix C: Trend Micro Services

Trend Micro Outbreak Prevention Policy C-2
Trend Micro Damage Cleanup Services C-2
The Damage Cleanup Services Solution C-2
Trend Micro Vulnerability Assessment C-3
Trend Micro IntelliScan C-4
Trend Micro ActiveAction C-4
Default ActiveAction Settings C-5
Trend Micro IntelliTrap C-6
True File Type C-6
Trend Micro Email Reputation Services C-7
Trend Micro Web Threat Protection C-7

Appendix D: Client Information

Roaming Clients D-2
32-bit and 64-bit Clients D-3

Appendix E: Spyware/Grayware Types

Appendix F: Glossary of Terms

Index

Preface

Welcome to the Trend Micro™ Worry-Free™ Business Security Advanced 5.1 Administrator's Guide. This book contains information about the tasks needed to install and configure Worry-Free Business Security Advanced.

The topics discussed in this chapter include:

- *Audience* on page xiv
- *Product Documentation* on page xiv
- *Document Conventions and Terms* on page xvii

Audience

This book is intended for novice and experienced Administrators of Worry-Free Business Security Advanced (WFBS-A) who want to configure, administer, and use the product.

Product Documentation

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

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

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

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

  Who should use the online help?

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

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

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

  http://www.trendmicro.com/download

  Who should read this guide?

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

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

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

  http://www.trendmicro.com/download

  Who should read this guide?

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

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

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

  http://esupport.trendmicro.com

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

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

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

What Information Can I Find in the Administrator's Guide?

This document can be separated into four main sections consisting of installation planning, product and component installation, post installation configuration, and finding help.

- **Chapters 1 and 2:** These chapters provide an overview of the key features and capabilities of Worry-Free Business Security Advanced.
- **Chapter 3:** This chapter explains the steps necessary for installing or upgrading Agents. It also provides information on removing the Agent.
- **Chapter 4:** This chapter explains the concept and usage of groups in Worry-Free Business Security Advanced.
- **Chapters 5 and 6:** These chapters explain the steps necessary for configuring groups.
- **Chapter 7:** This chapter explains the Outbreak Defense Strategy, how to configure Outbreak Defense, and how to use it to protect networks and Clients.
- **Chapter 8:** This chapter describes how to use Manual and Scheduled scans to protect your network and Clients from virus/malware and other threats.
- **Chapter 9:** This chapter explains how to use and configure Manual and Scheduled Updates.
- **Chapter 10:** This chapter describes how to use logs and reports to monitor your system and analyze your protection.
- **Chapter 11:** This chapter explains how to use the different notification options.
- **Chapter 12:** This chapter explains how to use Global Settings.
- **Chapter 13:** 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.
- **Chapter 14:** This chapter explains how to use the Administrative and Client tools that come with Worry-Free Business Security Advanced.
- **Chapter 15:** This chapter provides answers to commonly asked questions about installation and deployment, describes how to troubleshoot problems that may arise with Worry-Free Business Security Advanced, and provides information you will need to contact Trend Micro technical support.
- **Appendices:** These chapters include system check lists and the exclusion list for spyware/grayware, provide information on the various Trend Micro Services,

information about the Client, the different types of spyware/grayware, and a Glossary.

Document Conventions and Terms

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

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

CONVENTION/TERM	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation
`Monospace`	Sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip	Recommendations
WARNING!	Critical actions and configuration options
Navigation Path	The navigation path to reach a particular screen. For example, **Scans > Manual Scans**, means, click **Scans**, and then click **Manual Scans** on the interface.
Security Server	The Security Server hosts the Web console, the centralized Web-based management console for the entire Worry-Free Business Security Advanced solution.
Web console	The Web console is a centralized, Web-based, management console that manages all the Agents. The Web console resides on the Security Server.
Agent/CSA/MSA	The Client/Server Security Agent or Messaging Security Agent. 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 Client/Server Security Agent is installed.

Chapter 1

Introducing Worry-Free Business Security Advanced

This chapter provides an overview of Worry-Free Business Security Advanced's key features and capabilities.

The topics discussed in this chapter include:

- *Overview of Worry-Free Business Security Advanced* on page 1-2
- *What's New in This Release?* on page 1-2
- *What's Included in Worry-Free Business Security Advanced* on page 1-5
- *Understanding Threats* on page 1-12
- *How Worry-Free Business Security Advanced Protects Your Computers and Network* on page 1-17
- *What Else Can Worry-Free Business Security Advanced Do?* on page 1-21
- *Updateable Components* on page 1-28

Overview of Worry-Free Business Security Advanced

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

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

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

What's New in This Release?

What's New in Version 5.1

This version of Worry-Free Business Security Advanced brings a host of benefits to businesses that lack dedicated resources for antivirus management. Version 5.1 inherits all the features of previous versions and provides the following new features:

Support for Windows™ Small Business Server 2008

Version 5.1 supports Windows Small Business Server (SBS) 2008, allowing users to handle built-in security components in SBS 2008 and avoid conflicts. Version 5.1 handles SBS 2008 security features as follows:

- The Worry-Free Business Security Advanced installer prompts users to remove Microsoft™ Forefront™ Security for Exchange Server™ before continuing the installation.

- The Security Server installer does not disable or remove Microsoft Windows Live™ OneCare for Server; however, the installer for the Client/Server Security Agent (CSA) removes OneCare from client computers.

Version 5.1 also provides an add-in to the SBS console that allows administrators to view live security and system information.

Support for Windows™ Essential Business Server (EBS) 2008

Version 5.1 supports Windows Essential Business Server 2008, allowing users to install applicable Worry-Free Business Security Advanced components on computers handling the server roles that are supported by EBS 2008. Version 5.1 allows EBS 2008 administrators to:

- Install the Security Server on computers handling any server role.
- View live security and system information on the EBS console using the provided add-in.
- Install the Messaging Security Agent (MSA) on computers designated as messaging servers.
- Remove Microsoft™ Forefront™ Security for Exchange Server™ (Forefront) before continuing to install the MSA; the MSA installer prompts users to remove Forefront.

Support for Microsoft Exchange Server 2007 on Windows Server™ 2008

Version 5.1 includes a newer version of the Messaging Security Agent (MSA) that supports Exchange Server 2007 on Windows Server 2008.

Enhanced Security Engines

Version 5.1 includes the following new engines:

- Web Threat Protection (originally called "Web Reputation Services") engine with enhanced feedback mechanism supporting the Trend Micro Smart Protection Network for faster discovery and handling of unknown Web threats
- Scan engine with reduced memory footprint and other performance enhancements

- Behavior monitoring engine that provides threat deactivation, intelligent handling of dynamic ActiveX installations, and other features and enhancements

Additional Scan Information on the Security Groups Tree

Administrators can now see the date and time of the last manual and scheduled scans for the selected desktop or server group in the Security Groups tree.

What's New in Version 5.0

The following features were added in version 5.0:

Security Server

- **Location Awareness:** Worry-Free Business Security Advanced can identify the location of a Client based on Server Gateway information. Administrators can have different security settings based on the location of the Client (roaming or within the office).
- **Threat Status:** View Web Threat Protection and Behavior Monitoring statistics on the Live Status screen.
- **Plug-in Manager:** Add/remove plug-ins for Agents.
- **User Interface:** Security Server now comes with a new and improved user interface.

Client/Server Security Agent

- **Windows Vista Support:** Client/Server Security Agents can now be installed on Windows Vista (32-bit and 64-bit) computers. Refer to *32-bit and 64-bit Clients* on page D-3 for a comparison of the CSA features on different platforms.
- **Behavior Monitoring:** Behavior Monitoring protects Clients from unauthorized changes to the operating system, registry entries, other software, or files and folders.
- **Web Threat Protection:** Web Threat Protection (originally "Web Reputation Services") evaluates the potential security risk of each requested URL by querying the Trend Micro Security database at the time of each HTTP request.
- **Instant Message Content Filtering:** Instant Message Content Filtering can restrict the use of certain words or phrases while using instant messaging applications.

- **Software Protection:** With Software Protection, a user can restrict the applications that modify contents of folders on his/her computer.
- **POP3 Mail Scan:** POP3 Mail Scan protects Clients against security risks and spam transmitted through email messages.

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

- **TrendSecure™:** TrendSecure comprises a set of browser-based tools (TrendProtect and Transaction Protector) that enable users to surf the Web securely. TrendProtect warns users about malicious and Phishing Web sites. Transaction Protector determines the safety of your wireless connection by checking the authenticity of the access point.
- **Intuit™ Protection:** Protect all your QuickBooks files and folders from unauthorized changes by other programs.
- **Plug-in Manager Support:** Manage additional plug-ins for Client/Server Security Agent from the Security Server.
- **User Interface:** Client/Server Security Agent now comes with a new and improved user interface.

Messaging Security Agent

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

What's Included in Worry-Free Business Security Advanced

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

- Messaging Security Agent, which protects Microsoft Exchange servers, filters spam, and blocks content.

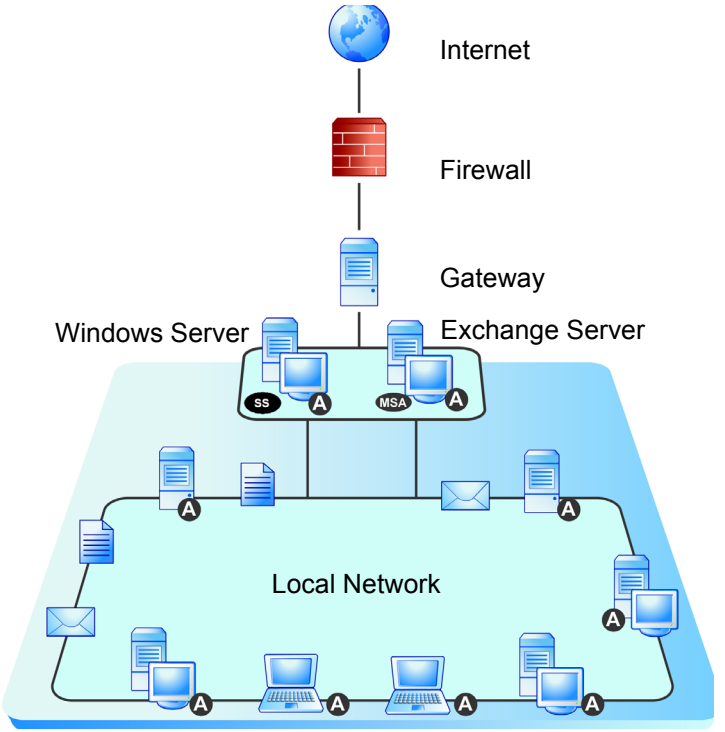


FIGURE 1-1. Worry-Free Business Security Advanced protects desktops, servers, and Microsoft Exchange servers

TABLE 1-1. Legend

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

Web Console

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

Also use the Web console to:

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

Security Server

At the center of Worry-Free Business Security Advanced is the Security Server (indicated by **SS** in Figure 1-1). The Security Server hosts the Web console, the centralized Web-based management console for Worry-Free Business Security Advanced. 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 Trend Micro Security Server performs these important functions:

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

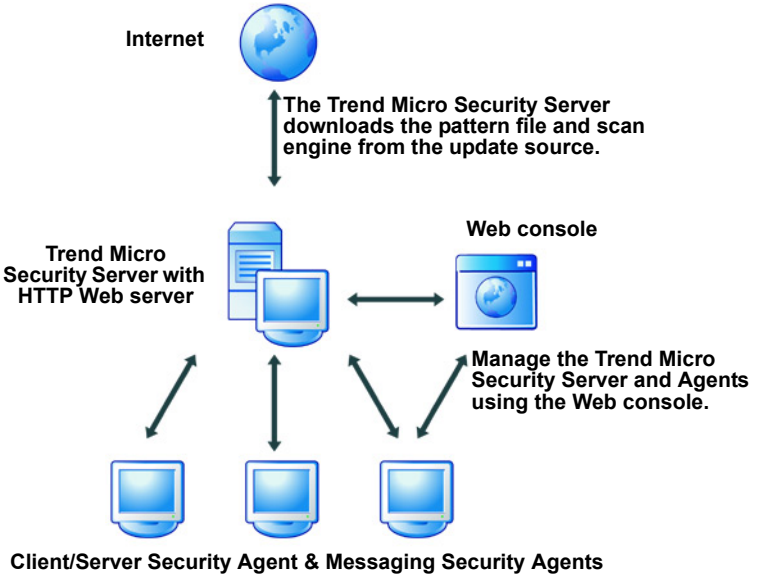


FIGURE 1-2. How Client/Server communication through HTTP works

Client/Server Security Agent

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

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

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

Messaging Security Agent

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

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

Scan Engine

At the heart of all Trend Micro products lies a scan engine. Originally developed in response to early file-based computer virus/malware, 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 virus/malware. The scan engine detects two types of threats:

- **Actively circulating:** Threats that are actively circulating on the Internet
- **Known and controlled:** Controlled virus/malware 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/malware would hide. If Worry-Free Business Security Advanced detects a virus/malware, 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. Worry-Free Business Security Advanced can also scan multiple layers of compression within a file (maximum of six).

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

- Frequent updates to the virus pattern file
- Upgrades to the engine software prompted by a change in the nature of virus/malware 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/malware 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/malware is discovered
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

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

http://www.trendmicro.com

Virus Pattern File

The Trend Micro Scan Engine uses an external data file, called the virus pattern file. It contains information that helps Worry-Free Business Security Advanced identify the latest virus/malware and other Internet threats such as Trojan horses, mass

mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly threat is discovered.

All Trend Micro antivirus programs using the ActiveUpdate function can detect the availability of a new virus pattern file on the Trend Micro server. Administrators can schedule the antivirus program to poll the server every week, day, or hour to get the latest file.

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

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

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

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

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

Virus Cleanup Engine

WFBS-A makes use of a scanning and cleanup tool called the Virus Cleanup Engine to find and repair damage caused by virus/malware and other Internet threats. The Virus Cleanup Engine can find and clean virus/malware, Trojans, and other threats. The Virus Cleanup Engine makes use of a database to find targeted machines and evaluate whether threats have affected them. The Virus Cleanup Engine resides on a single machine and deploys to the targeted Client on the network at the time of scanning.

The Virus Cleanup Engine uses the Virus Cleanup Pattern to restore damage caused by the latest known threats. WFBS-A regularly updates these templates. Trend Micro recommends to update the components immediately after installing and activating WFBS-A. Trend Micro updates the Virus Cleanup Pattern frequently.

Common Firewall Driver

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

Network Virus Pattern File

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

Vulnerability Pattern File

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

Understanding Threats

Computer security is a rapidly changing subject. Administrators and information security professionals invent and adopt a variety of terms and phrases to describe potential risks or uninvited incidents to computers and networks. The following is a discussion of these terms and their meanings as used in this document.

Virus/Malware

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

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

- **Malware:** Malware is software designed to infiltrate or damage a computer system without the owner's informed consent.
- **Trojans:** A Trojan is a malicious program that masquerades as a harmless application. Unlike virus/malware, Trojans do not replicate but can be just as destructive. An application that claims to rid your computer of virus/malware when it actually introduces virus/malware into your computer is an example of a Trojan.
- **Worms:** A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments. Unlike virus/malware, worms do not need to attach themselves to host programs.
- **Backdoors:** A backdoor is a method of bypassing normal authentication, securing remote access to a computer, and/or obtaining access to information, while attempting to remain undetected.
- **Rootkit:** A rootkit is a set of programs designed to corrupt the legitimate control of an operating system by its users. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security.
- **Macro Viruses:** Macro viruses are application-specific. The viruses reside within files for applications such as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications such as .doc, .xls, and .ppt. Macro viruses travel amongst data files in the application and can eventually infect hundreds of files if undeterred.

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

Spyware/Grayware

Grayware is a program that performs unexpected or unauthorized actions. It is a general term used to refer to spyware, adware, dialers, joke programs, remote access

tools, and any other unwelcome files and programs. Depending on its type, it may or may not include replicating and non-replicating malicious code.

- **Spyware:** Spyware is computer software that is installed on a computer without the user's consent or knowledge and collects and transmits personal information.
- **Dialers:** Dialers are necessary to connect to the Internet for non-broadband connections. Malicious dialers are designed to connect through premium-rate numbers instead of directly connecting to your ISP. Providers of these malicious dialers pocket the additional money. Other uses of dialers include transmitting personal information and downloading malicious software.
- **Hacking Tools:** A hacking tool is a program, or a set of programs, designed to assist hacking.
- **Adware:** Adware, or advertising-supported software, is any software package, which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- **Keyloggers:** A keylogger is computer software that logs all the keystrokes of the user. This information could then be retrieved by a hacker and used for his/her personal use.
- **Bots:** A bot (short for "robot") is a program that operates as an agent for a user or another program or simulates a human activity. Bots, once executed, can replicate, compress, and distribute copies of themselves. Bots can be used to coordinate an automated attack on networked computers.

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

Network Viruses

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

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

Spam

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

Intrusions

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

Malicious Behavior

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

Fake Access Points

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

Explicit/Restricted Content in IM Applications

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

Online Keystroke Listeners

An online version of a keylogger. See *Spyware/Grayware* on page 1-13 for more information.

Packers

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

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

Phishing Incidents

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

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

Mass-Mailing Attacks

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

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

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

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

TABLE 1-2. Threats and Worry-Free Business Security Advanced Protection

Threat	Worry-Free Business Security Advanced Protection
• **Virus/Malware.** Virus, Trojans, Worms, Backdoors, and Rootkits • **Spyware/Grayware.** Spyware, Dialers, Hacking tools, Password cracking applications, Adware, Joke programs, and Keyloggers	Antivirus and Anti-spyware Scan Engines along with Pattern Files in Client/Server Security Agent and Messaging Security Agent
Virus/Malware and Spyware/Grayware transmitted through email messages and spam	POP3 Mail Scan in Client/Server Security Agent and IMAP Mail Scan in Messaging Security Agent
Network Worms/Viruses	Firewall in Client/Server Security Agent
Intrusions	Firewall in Client/Server Security Agent
Conceivably harmful Web sites/Phishing sites	Web Threat Protection and TrendProtect in Client/Server Security Agent
Malicious behavior	Behavior Monitoring in Client/Server Security Agent
Fake access points	Transaction Protector in Client/Server Security Agent
Explicit/restricted content in IM applications	IM Content Filtering in Client/Server Security Agent

About Components

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

Antivirus

- **Scan Engine (32-bit/64-bit) for Client/Server Security Agent and Messaging Security Agent:** The scan engine uses the virus pattern file to detect virus/malware and other security risks on files that your users are opening and/or saving.
  The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique "signature" or string of tell-tale characters that distinguish it from any other code, the virus experts at Trend Micro capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to patterns in the virus pattern file, searching for a match.
- **Virus Pattern:** A file that helps the Security Agents identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.
- **Virus Cleanup Template:** Used by the Virus Cleanup Engine, this template helps identify Trojan files and Trojan processes, worms, and spyware/grayware so the engine can eliminate them.
- **Virus Cleanup Engine (32-bit/64-bit):** The engine that Cleanup Services uses to scan for and remove Trojan files and Trojan processes, worms, and spyware/grayware.
- **IntelliTrap Exception Pattern:** The exception pattern used by IntelliTrap and the scan engines to scan for malicious code in compressed files.
- **IntelliTrap Pattern:** The pattern used by IntelliTrap and the scan engines to scan for malicious code in compressed files.

Anti-spyware

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

- **Spyware Active-monitoring Pattern:** Similar to the spyware pattern, but is used by the scan engine for real-time anti-spyware scanning.

Anti-spam

- **Spam engine (32-bit/64-bit):** Detects unsolicited commercial email messages (UCEs) or unsolicited bulk email messages (UBEs), otherwise known as spam.
- **Spam Pattern:** Contains spam definitions to enable the anti-spam engine to detect spam in email messages.
- **Email Reputation Services (ERS):** Stops up to 80 percent of spam before it hits the gateway and floods the messaging infrastructure.

Outbreak Defense

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

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

Firewall

- **Common Firewall Engine (32-bit/64-bit):** The Firewall uses this engine, together with the network virus pattern file, to protect computers from hacker attacks and network viruses.
- **Common Firewall Pattern:** Like the virus pattern file, this file helps Worry-Free Business Security Advanced identify network virus signatures.
- **Transport Driver Interface (TDI) (32-bit/64-bit):** The module that redirects network traffic to the scan modules.
- **WFP Driver (32-bit/64-bit):** For Windows Vista Clients, the Firewall uses this driver with the network virus pattern file to scan for network viruses.

Web Threat Protection

- **Trend Micro Security database:** Web Threat Protection evaluates the potential security risk of the requested Web page before displaying it. Depending on rating

returned by the database and the security level configured, Client/Server Security Agent will either block or approve the request.

- **URL Filtering Engine (32-bit/64-bit):** The engine that queries the Trend Micro Security database to evaluate the page.

TrendProtect

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

Software Protection

Software Protection List: The Software Protection List comprises programs that can modify the contents of files or folders. If a program is not in the list, it cannot create, modify, or delete files or folders.

Behavior Monitoring

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

Transaction Protector

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

Content Filtering

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

Live Status and Notifications

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

Other Supplementary Trend Micro Products

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

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

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

What Else Can Worry-Free Business Security Advanced Do?

With Worry-Free Business Security Advanced, Administrators can also:

- *Manage Security From a Single Console* on page 1-22
- *Analyze Network Protection* on page 1-22
- *Enforce Security Policies* on page 1-22
- *Have Updated Protection* on page 1-23
- *Quarantine Infected Files* on page 1-23

- *Control Outbreaks on the Network* on page 1-23
- *Manage Worry-Free Business Security Advanced Groups* on page 1-23
- *Protect Clients from Hacker Attacks with Firewall* on page 1-24
- *Protect Email Messages* on page 1-24
- *Filter Instant Messaging Content* on page 1-24
- *Control Security Settings Based on Location* on page 1-24
- *Protect Clients from Visiting Malicious Web Sites* on page 1-26
- *Facilitate Safe Online Transactions* on page 1-27
- *Approved Spyware/Grayware Programs* on page 1-27
- *Secure Communication* on page 1-28

Manage Security From a Single Console

The Trend Micro Security Server manages the entire antivirus system through a single Web console known as the Web console. Web console is installed along with the Trend Micro Security Server and uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

Analyze Network Protection

Worry-Free Business Security Advanced can generate various types of logs, including virus/malware logs, system event logs, and update logs. Use these logs to verify update deployment, check client-server communication, and determine which computers are vulnerable to infection.

Also use log information as a basis for designing and redesigning network protection, identifying which computers are at a higher risk of infection and changing the antivirus settings accordingly for these computers.

Enforce Security Policies

Worry-Free Business Security Advanced provides three types of scans: Scheduled Scan, Manual Scan, and Real-time Scan. Enforce the organization's security policies by configuring these three types of scans. Specify the types of files to scan and the action to take when Worry-Free Business Security Advanced finds a threat.

To apply regulated scan settings to all Agents, choose not to grant privileges to users and lock the Agent with a password to prevent users from altering settings, turning off, or removing protection.

Have Updated Protection

Virus writers create new virus/malware and release them frequently. To stay protected against the latest threats, Trend Micro releases new virus pattern files frequently. Worry-Free Business Security Advanced can automatically download and deploy the pattern files to all the agents.

Quarantine Infected Files

Specify a quarantine folder to control live virus/malware and infected files. The Trend Micro Security Server then automatically moves infected files to the quarantine folder.

Control Outbreaks on the Network

Respond immediately to developing outbreaks by enabling Outbreak Defense and setting up outbreak notifications.

Outbreak Defense helps stop outbreaks from overwhelming the network by:

- blocking shared folders and vulnerable ports on Clients
- denying write access to folders
- blocking attachments and filtering content

Manage Worry-Free Business Security Advanced Groups

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

Protect Clients from Hacker Attacks with Firewall

Help protect Clients from hacker attacks and network viruses by creating a barrier between the Client and the network. Firewall can block or allow certain types of network traffic. Additionally, Firewall will identify patterns in network packets that may indicate an attack on Clients.

Protect Email Messages

POP3 Email Messages

Protects Clients running Windows 2000/XP/Server 2003 from infected Post Office Protocol 3 (POP3) mail messages and attachments and spam. When a threat is detected, the user can choose to delete, clean, or ignore the mail message containing the threat.

IMAP Email Messages

Worry-Free Business Security Advanced offers powerful scanning technology that can detect, clean/quarantine, a wide variety of threats. It also offers attachment blocking, content filtering, and other features; all accessible from the Web console.

Filter Instant Messaging Content

With IM Content Filtering, Administrators can restrict the usage of certain words transmitted through popular instant messaging applications.

Refer to *IM Content Filtering* on page 12-8 for more details.

Control Security Settings Based on Location

With Location Awareness, Administrators can control security settings depending on how the Client is connected to the network.

For example, if a person is not in the office, Administrators can set more rigid policies and enable the firewall. But, if the person is at work, the firewall can be disabled.

Client/Server Security Agents can have different profiles depending on their location. WFBS-A classifies Clients as:

- Normal Clients
- Roaming Clients

Normal Clients

Normal Clients are computers that are stationary and maintain a continuous network connection with the Security Server.

Roaming Clients

Roaming Clients are computers that do not always maintain a constant network connection with the Security Server, such as portable computers. These Clients' Client/Server Security Agents continue to provide virus/malware protection, but have delays in sending their status to the Security Server.

Roaming privileges are normally assigned to Clients that are disconnected from the Security Server for an extended period. When a Client is granted roaming privileges, it can update itself directly from the Trend Micro ActiveUpdate server. Clicking **Update Now** on the Client/Server Security Agent shortcut menu.

Location Awareness controls the In Office/Out of Office connection settings. Refer to *Location Awareness* on page 12-5.

Behavior Monitoring

Behavior Monitoring constantly monitors the Client for attempts to modify the operating system and other programs. When the Agents detect an attempt, it notifies the user of the change and the user can Allow or Block the request. Users/administrators can add programs into an exception list. Programs in the exception list can make changes to other programs and the operating system.

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.

Protect Clients from Visiting Malicious Web Sites

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

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

Web Threat Protection provides both email notification to the Administrator and online notification to the user for Web Threat Protection detections.

Refer to *Web Threat Protection* on page 5-15 to configure Web Threat Protection.

Reputation Score

A URL's "reputation score" determines whether a URL 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 Agents will allow or block access to a URL.

- **High:** Blocks URLs that are unrated, a Web threat, very likely to be a Web threat, or likely to be a Web threat.
- **Medium:** Blocks URLs that are unrated, a Web threat, or very likely to be a Web threat.
- **Low:** Blocks only URLs that are a Web threat.

Refer to *Web Threat Protection* on page 12-7 and *Web Threat Protection* on page 5-15 for more information.

Facilitate Safe Online Transactions

TrendSecure helps safeguard your Internet transactions by determining the safety of your wireless connection and the Web page you are visiting.

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

- **Wi-Fi Advisor:** Checks the safety of wireless networks based on the validity of their SSIDs, authentication methods, and encryption requirements.
- **Page Ratings:** Determines the safety of the hyperlinks on a page (applicable for wireless and wired connections).

Refer to *TrendSecure* on page 5-21 for more information.

Approved Spyware/Grayware Programs

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

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

If users require Hotbar or any other application that Worry-Free Business Security Advanced classifies as spyware/grayware, add it to the spyware/grayware approved list. Refer to *Editing the Spyware/Grayware Approved List* on page 8-6 for more information.

By preventing potentially risky applications from running and by giving full control over the spyware/grayware approved list, Worry-Free Business Security Advanced helps ensure that only approved applications run on Clients.

Secure Communication

Worry-Free Business Security Advanced provides secure communications between the Trend Micro Security Server and the Web console through Secure Socket Layer (SSL) technology.

The Trend Micro Security Server can generate a certificate for each session, allowing the Web console to encrypt data based on Public Key Infrastructure (PKI) cryptography standards. The default period for the certificate is three years.

Updateable Components

To ensure Worry-Free Business Security Advanced uses the latest components to scan for, identify, and clean Clients, Trend Micro updates the following regularly:

- **Components:** Refer to *About Components* on page 1-17 and *Updatable Components* on page 9-3 for more information.
- **Hot fixes and security patches:** Workaround solutions to customer related problems or newly discovered security vulnerabilities that can be downloaded from the Trend Micro Web site and installed to the Trend Micro Security Server and/or Agent

Refer to *About Components* on page 1-17 for information about each component.

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.

Obtain hot fixes from your Technical Account Manager. Check the Trend Micro Knowledge Base to search for released hot fixes:

http://esupport.trendmicro.com/support

Check the Trend Micro Web site regularly to download patches and service packs:

http://www.trendmicro.com/download

Note: 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.

Chapter 2

Working With the Web Console

This chapter tells you how to get up and running with Worry-Free Business Security Advanced.

The topics discussed in this chapter include:

- *Exploring the Web Console* starting on page 2-2
- *Using Live Status and Notifications* starting on page 2-6

Exploring the Web Console

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

To open the Web console:

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

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

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

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

---

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

FIGURE 2-1. Logon screen of Worry-Free Business Security Advanced

3. Type your password in the **Password** text box, and then click **Log on**. The browser displays the **Live Status** screen of the Web console. See *Using Live Status* on page 2-7.

Web Console Features

The following is a description of the major features of the Web console.

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, 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. Refer to *Security Settings Toolbar* on page 4-5 for more information.

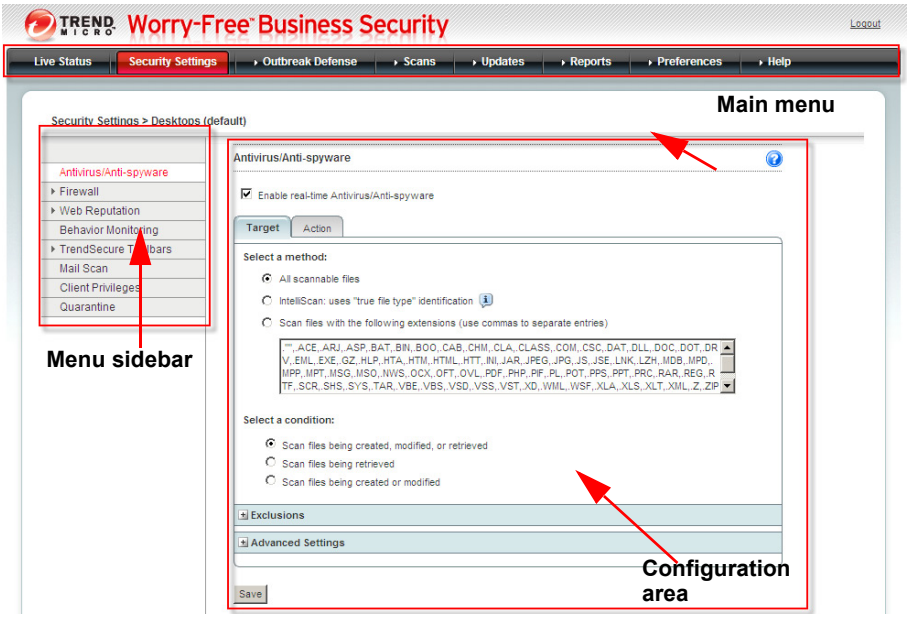


FIGURE 2-2. Web console Overview

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.

Using Live Status and Notifications

When Worry-Free Business Security Advanced detects a significant threat or system event, it displays the results in the **Live Status** screen (see Figure 2-3 on page 2-8). You can set Worry-Free Business Security Advanced to send notifications whenever these events happen. In addition, you can customize the parameters that trigger notifications and appear on the **Live Status** screen.

Setting Up Notifications

Use **Preferences > Notifications** to set up event notifications or customize parameters for the events. Refer to *Working with Notifications* on page 11-1 for more information.

Trend Micro recommended settings for Notifications

By default, all events listed on the **Notifications** screen are selected and trigger the Security Server to send a notification to the Administrator.

Click a notification to display the notification content detail and customize the details, if necessary.

The following settings are the default values used by Worry-Free Business Security Advanced.

- **Antivirus**
  Virus/malware detected on desktops/servers exceeds 5 incidents within 1 hour

  Virus/malware detected on Microsoft Exchange servers exceeds 10 incidents within 1 hour
- **Anti-spyware**
  Spyware/grayware detected on desktops/servers exceeds 15 incidents within 1 hour
- **Anti-spam**
  Spam exceeds 10% of total messages
- **Web Threat Protection**
  URL violation exceeds 200 incidents within 1 hour
- **Behavior Monitoring**
  Policy violation exceeds 20 incidents within 1 hour

- **Network Virus**
  Network viruses detected exceeds 10 incidents within 1 hour
- **Unusual System Events**
  The available free disk space is decreasing to less than 1%

Using Live Status

The **Live Status** screen is the first screen that displays when opening the Web console. All the information you need to know is displayed on one screen.

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

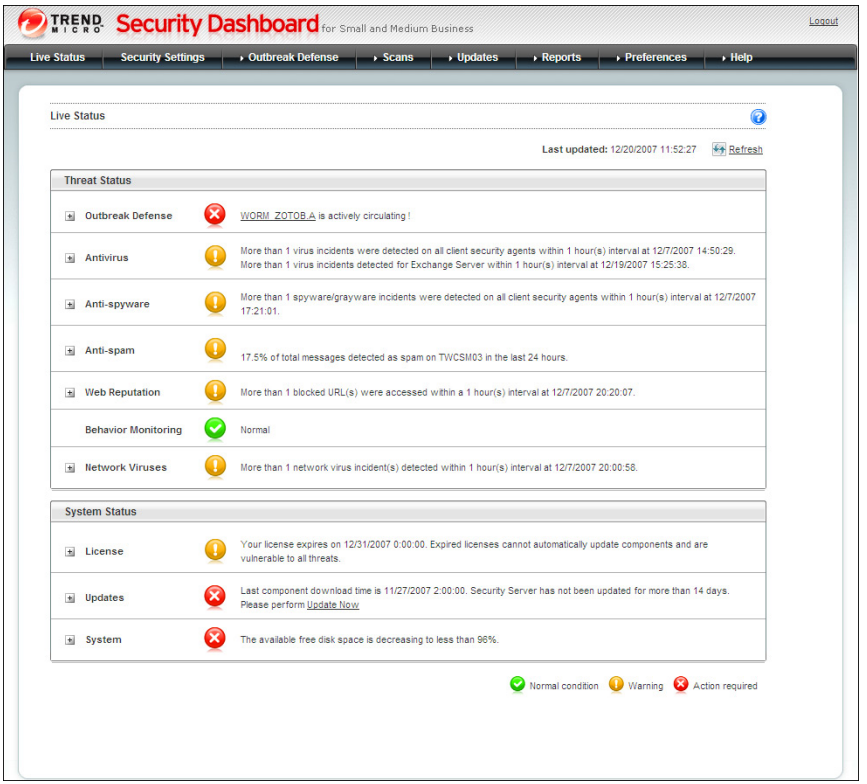


FIGURE 2-3. Live Status screen

Understanding Icons

The Live Status screen depicts the status of threats and the system using icons. The following table describes what the different icons means:

TABLE 2-3. Live Status Icons

Icon	Description
	No action required 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 (refer to *Yellow Alerts* on page 2-13) is issued by Trend Micro, the warning displays for Outbreak Defense. Click ([+]) next to the warning icon to view detailed information. Click the underlined links to display detailed information and take further actions.
	Action required Typically, a warning icon means that you have many vulnerable computers that are reporting too many virus or spyware incidents. When a Red Alert (refer to *Red Alerts* on page 2-12) is issued by Trend Micro, the warning displays for Outbreak Defense. Click ([+]) next to the warning icon to view detailed information. Click the underlined links to display detailed information and take further actions.

Beside each of the items on the **Live Status** screen is an icon ([+]). Clicking the icon reveals a panel of information about that item. From the expanded panel you can click links to be redirected to other screens where you can take actions to resolve problems specific to that panel.

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

Threat Status

Threat Status, part of the **Live Status** screen, reports security risks on your network based on Trend Micro recommended policies. The icons warn you if action is necessary to secure the Clients on your network. Expand a section to view more information. You can also click the items in the table to view specific details.

By default, the information is refreshed every hour. To manually refresh the information, click Refresh ().

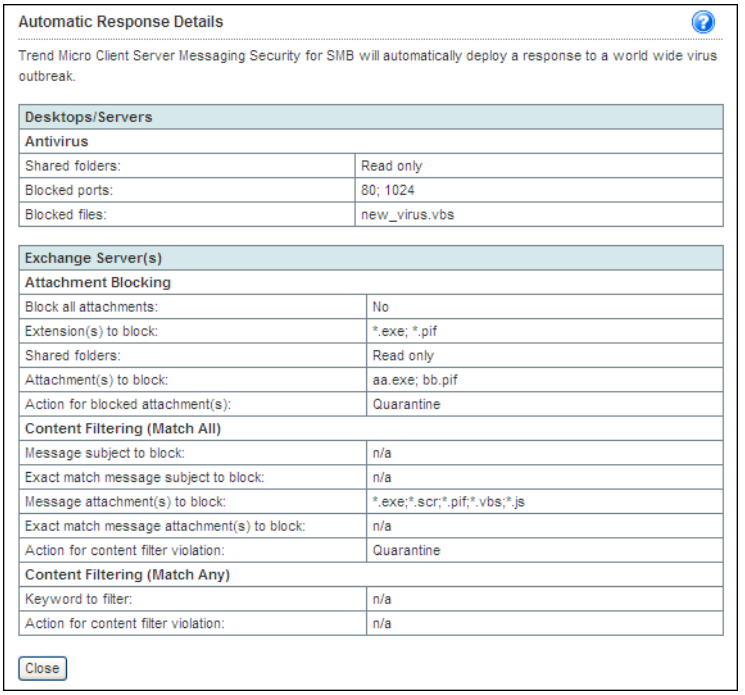
The following threats are displayed on the **Live Status** screen:

- *Outbreak Defense* on page 2-10
- *Red Alerts* on page 2-12
- *Yellow Alerts* on page 2-13
- *Antivirus* on page 2-13
- *Anti-spyware* on page 2-13
- *Anti-spam* on page 2-13
- *Web Threat Protection* on page 2-14
- *Behavior Monitoring* on page 2-14
- *Network Viruses* on page 2-14

Outbreak Defense

The Security Server determines whether your network has an outbreak problem based on policies that it downloads from Trend Micro. When there is a problem, the Security Server displays a red (dangerous) or yellow (warning) alert icon and triggers Outbreak Defense. During Outbreak Defense, the Security Server might take protective actions such as blocking ports, downloading components, and running

scans. You can view these actions by clicking **View** from the **Threat Information** section in **Outbreak Defense > Current Status**.



Automatic Response Details

Trend Micro Client Server Messaging Security for SMB will automatically deploy a response to a world wide virus outbreak.

Desktops/Servers	
Antivirus	
Shared folders:	Read only
Blocked ports:	80; 1024
Blocked files:	new_virus.vbs

Exchange Server(s)	
Attachment Blocking	
Block all attachments:	No
Extension(s) to block:	*.exe; *.pif
Shared folders:	Read only
Attachment(s) to block:	aa.exe; bb.pif
Action for blocked attachment(s):	Quarantine
Content Filtering (Match All)	
Message subject to block:	n/a
Exact match message subject to block:	n/a
Message attachment(s) to block:	*.exe;*.scr;*.pif;*.vbs;*.js
Exact match message attachment(s) to block:	n/a
Action for content filter violation:	Quarantine
Content Filtering (Match Any)	
Keyword to filter:	n/a
Action for content filter violation:	n/a

Close

FIGURE 2-4. Automatic Response Details

During an outbreak alert, clicking the underlined link from the **Vulnerable Computers** or **Computers to Cleanup** section opens the **Current Threat** screen to show you how the Security Server is protecting your Clients and network. Under normal conditions, clicking these links opens the **Potential Threats** screen where

you can view at-risk Clients and initiate scanning to check for vulnerabilities and clean damaged Clients. See *Outbreak Defense Strategy* on page 7-2.

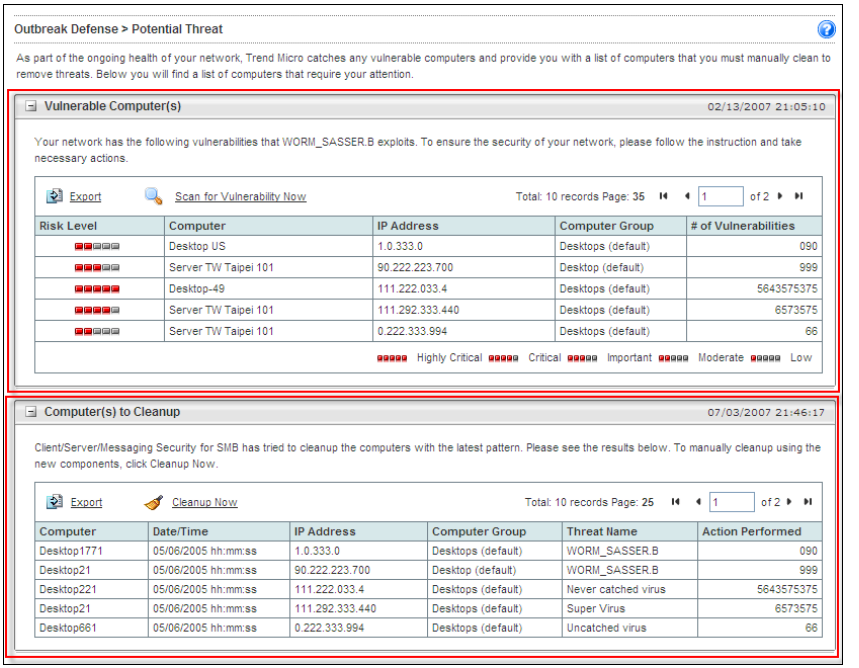


FIGURE 2-5. Outbreak Defense > Potential Threat screen

Red Alerts

Several infection reports from each business unit reporting rapidly spreading virus/malware, where gateways and email servers may need to be patched. The industry's first 45-minute Red Alert solution process starts: An official pattern release (OPR) is deployed with notification of its availability, any other relevant notifications are sent out, and fix tools and information regarding vulnerabilities are posted on the download pages.

Yellow Alerts

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

Antivirus

The Antivirus section displays information from the latest virus scan and virus log entries. The **Number of Incidents** column on the **Virus Threat Incidents** table displays the results of the latest virus scan.

Anti-spyware

The Anti-spyware section displays the number of Spyware/Grayware Threat Incidents within a certain specified period. The Anti-spyware section also displays the number of Clients that need to be restarted in order to finish the spyware/grayware cleaning process.

Anti-spam

The Anti-spam section displays information relating to spam activity on Microsoft Exchange servers. Live Status displays information about the current spam threshold level and the amount of spam that the Microsoft Exchange servers are receiving.

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. The detection level determines how tolerant Messaging Security Agent will be towards suspect email messages.

- **High:** This is the most rigorous level of spam detection. The MSA 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 MSA filters as spam when they are actually legitimate email messages.
- **Medium:** This is the default setting. The MSA 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 MSA will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives.

Note: This information is updated on an hourly basis. For the latest information, generate a report. Refer to *Generating Reports* on page 10-7 for more information.

Web Threat Protection

This information is generated based on the number of restricted URLs users visit. When the number of URLs visited exceeds the threshold, the status icon changes.

Behavior Monitoring

This information is generated based on the number of Behavior Monitoring policy violations on Clients. When the violations count exceeds the threshold, the status icon changes.

Network Viruses

The information displayed in the Network virus section is generated by the Firewall settings. When a Manual, Scheduled, or Real-time Scan detects a network virus, the information will be displayed in the Network Viruses section of the **Live Status** screen.

System Status

View information regarding the license status, updated components, and the free space on servers where Agents are installed.

License

The License section of the **Live Status** screen displays information about the status of your product license, specifically expiration information. To view details about your product license, click the **Product License** link. From the **Product License** screen, you can upgrade or renew your product.

Updates

The Updates section displays information about the status of component updates for the Security Server or the deployment of updated components to Agents. By default, Worry-Free Business Security Advanced downloads components from the Trend Micro ActiveUpdate Server and then makes them available to Agents. Agents download components from the Security Server (that is, the Security Server deploys the component to Agents).

- To deploy updated components to Agents, click **Deploy Now**
- To manually update the Security Server components from the ActiveUpdate Server, click **Update Now**

Unusual System Events

The System section displays disk space information about Clients that are functioning as servers (running server operating systems). Client/Server Security Agent reports the amount of free disk space available for use on the servers.

Chapter 3

Installing Agents

This chapter explains the steps necessary for installing or upgrading Agents. It also provides information on removing the Agent.

The topics discussed in this chapter include:

- *Choosing an Installation Method* on page 3-2
- *Installing, Upgrading, or Migrating Client/Server Security Agents* on page 3-3
- *Agent System Requirements* on page 3-4
- *Performing a Fresh Install* on page 3-5
- *Verifying the Agent Installation, Upgrade, or Migration* on page 3-17
- *Testing the Client Installation with the EICAR Test Script* on page 3-19
- *Removing Agents* on page 3-21

Choosing an Installation Method

Worry-Free Business Security Advanced provides several methods to install the Client/Server Security Agent. This section provides a summary of the different methods.

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

- **Internal Web page:** Instruct the users in your organization to go to the internal Web page and download the Client/Server Security Agent setup files (see *Installing from an Internal Web Page* on page 3-6)
- **Login Script Setup:** Automate the installation of the Client/Server Security Agent to unprotected computers when they log on to the domain (see *Installing with Login Script Setup* on page 3-7)
- **Client Packager:** Deploy the Client/Server Security Agent setup or update files to Clients through email (see *Installing with Client Packager* on page 3-9)
- **Remote Install:** Install the Agent on all Windows Vista/2000/XP/Server 2003/Server 2008 Clients from the Web console (see *Installing with Remote Install* on page 3-12)
- **Vulnerability Scanner (TMVS):** Install the Client/Server Security Agent on all Windows Vista/2000/XP (Professional)/Server 2003/Server 2008 Clients with the Trend Micro Vulnerability Scanner (*Installing with Vulnerability Scanner* on page 3-14)

TABLE 3-1. Trend Micro Client/Server Security Agent Deployment Methods

	Web page	Login scripts	Client packager	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
Bandwidth consumption	Low, if scheduled	High, if Clients are started at the same time	Low, if scheduled	Low, if scheduled	Low, if scheduled
Required Privileges	Administrator privileges required for all installation methods.				

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

Installing, Upgrading, or Migrating Client/Server Security Agents

This section provides information on the following:

- *Agent System Requirements* on page 3-4
- Performing a fresh Client/Server Security Agent install with your chosen installation method (see *Choosing an Installation Method* on page 3-2)

- Upgrading from a previous version of Client/Server 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 Worry-Free Business Security Advanced (see *Verifying the Agent Installation, Upgrade, or Migration* on page 3-17)

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

Agent System Requirements

The following table describes the minimum system requirements for Client/Server Security Agents:

TABLE 3-2. Installation requirements

Requirement	Minimum Specifications
Processor	• Intel™ Pentium™ x86 or compatible processor • x64 processor supporting AMD64 and Intel EM64T technologies Clock speed requirements vary depending on the operating system: • 1GHz (Windows Server® 2008, SBS 2008, or EBS 2008) • 800MHz (Windows Vista®) • 450MHz (Windows® 2000, SBS 2000, XP, Server 2003, SBS 2003, or Home Server)
Memory	• 512MB (x86 systems) • 1GB (x64 systems) • 4GB (Windows Essential Business Server 2008 or Windows Small Business Server 2008 systems)
Disk space	300MB

TABLE 3-2. Installation requirements (Continued)

Requirement	Minimum Specifications	
Operating system	**Series or Family**	**Supported Service Packs or Releases**
	Windows 2000	SP2, SP3, or SP4
	Windows Small Business Server (SBS) 2000	No service pack or SP1a
	Windows XP	No service pack, SP1, SP2, or SP3
	Windows Server 2003 (includes Storage Server 2003)	No service pack, SP1, R2, or SP2
	Windows SBS 2003	No service pack, SP1, R2, or SP2
	Windows Vista	No service pack or SP1
	Windows Home Server	No service pack
	Windows Server 2008	No service pack
	Windows SBS 2008	No service pack
	Windows Essential Business Server (EBS) 2008	No service pack
	Note: All major editions and 64-bit versions of these operating systems are supported unless noted otherwise.	
Web browser (for Web-based setup)	Internet Explorer 5.5 SP2 or later	
Display	256-color display or higher with resolutions of 800x600 or higher	

Performing a Fresh Install

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

Installing from an Internal Web Page

If you installed the Trend Micro Security Server to a computer running Windows 2000, Windows XP, or Windows Server 2003 with Internet Information Server (IIS) 5.0 or 6.0, or Apache 2.0.54, users can install the Client/Server Security Agent from the internal Web site created during master setup.

This is a convenient way to deploy the Client/Server Security Agent. You only have to instruct users to go to the internal Web page and download the Client/Server 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 *Using Vulnerability Scanner to Verify the Client Installation* on page 3-17 for more information).

Users must have Microsoft Internet Explorer 5.5 or later with the security level set to allow ActiveX controls to successfully download the Client/Server Security Agent setup files. The instructions below are written from the user perspective. Email your users the following instructions to install the Client/Server 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
   ```

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

2. Click **Install Now** to start installing the Client/Server 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 Client/Server Security Agent icon appears in the Windows system tray.

Installing with Login Script Setup

Use Login Script Setup to automate the installation of the Client/Server 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 Client/Server 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.

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

1. On the computer where you installed Worry-Free Business Security Advanced, 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 2000/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 Windows 2000/Server 2003/Server 2008 Scripts

If you already have an existing login script, 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 Windows 2000 login script is on the Windows 2000 server (through a net logon shared directory), under:

```
\\Windows 2000 server\{system drive}\WINNT\SYSVOL\
domain\scripts\ofcscan.bat
```

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
```

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. Client/Server Security 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.

Note: Client packager requires a minimum of 370MB free disk space on the Client. Windows Installer 2.0 is necessary for the Client to run an MSI package.

Client Packager can create two types of self-extracting files:

- **Executable**

  Note: In Windows Vista, the program must be executed with Administrator rights (Run as Administrator).

- **Microsoft Installer Package Format (MSI):** This file type 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 Web site.

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. In **Target operating system**, select the operating system for which you want to create the package.
5. Select the type of package you want to create:
   - **Setup:** Select if installing the Agent.
   - **Update:** Select if updating Client/Server Security Agent components only.
6. 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 Worry-Free Business Security Advanced performs before starting setup.
7. Under **Components**, select the components to include in the installation package:
   - **Program:** All components
   - **Scan engine:** The latest Scan Engine on the Trend Micro Security Server

- **Virus pattern:** The latest Virus Pattern File on the Trend Micro Security Server
- **Vulnerability pattern:** The latest Vulnerability Pattern File on the Trend Micro Security Server.
- **Spyware components:** The latest Spyware components on the Trend Micro Security Server.
- **Common Firewall Driver:** The driver for Firewall
- **Network Virus Pattern:** The latest pattern file specifically for network viruses
- **DCE/DCT:** The latest Virus Cleanup Engine and template on the Trend Micro Security Server
- **IntelliTrap pattern:** The latest IntelliTrap Pattern File on the Trend Micro Security Server.

8. 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.
9. In **Output file**, click ... to specify the file name (for example, `ClientSetup.exe`) and the location to create the package.
10. 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.
11. 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 the Client/Server Security Agents that report to the server where the package was created. Do not send the package to Client/Server 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 Client/Server 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 Client/Server Security Agent themselves.

For more information on MSI, see the Microsoft Web site (www.microsoft.com). 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 Client/Server Security Agent to multiple Windows Vista, 2000, 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 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).

To install CSA with Remote Install:

Note: Installing Client/Server Security Agent on Windows Vista requires a few additional steps. Refer to *Enabling Client/Server Security Agent Remote Install on Windows Vista Clients* on page 3-13 for additional details.

---

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 Client/Server 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 Client/Server Security Agent files to each target computer.

When Worry-Free Business Security Advanced 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 Client/Server Security Agent on a machine already running a Trend Micro Security Server.

Enabling Client/Server Security Agent Remote Install on Windows Vista Clients

Installing Client/Server Security Agent 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 Client/Server Security Agent 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 Client/Server 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, refer to *Using Vulnerability Scanner to Verify the Client Installation* on page 3-17.

Note: You can use Vulnerability Scanner on machines running Windows 2000 or Server 2003; however, the machines should not be running Terminal Server.
You cannot install the Client/Server 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 Client/Server Security Agent with Vulnerability Scanner:

1. In the drive where you installed the Trend Micro Security Server, go to the following location: Worry-Free Business Security Advanced > **PCCSRV** > **Admin** > **Utility** > **TMVS**. Double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears.

2. Click **Settings**. The **Settings** screen appears.

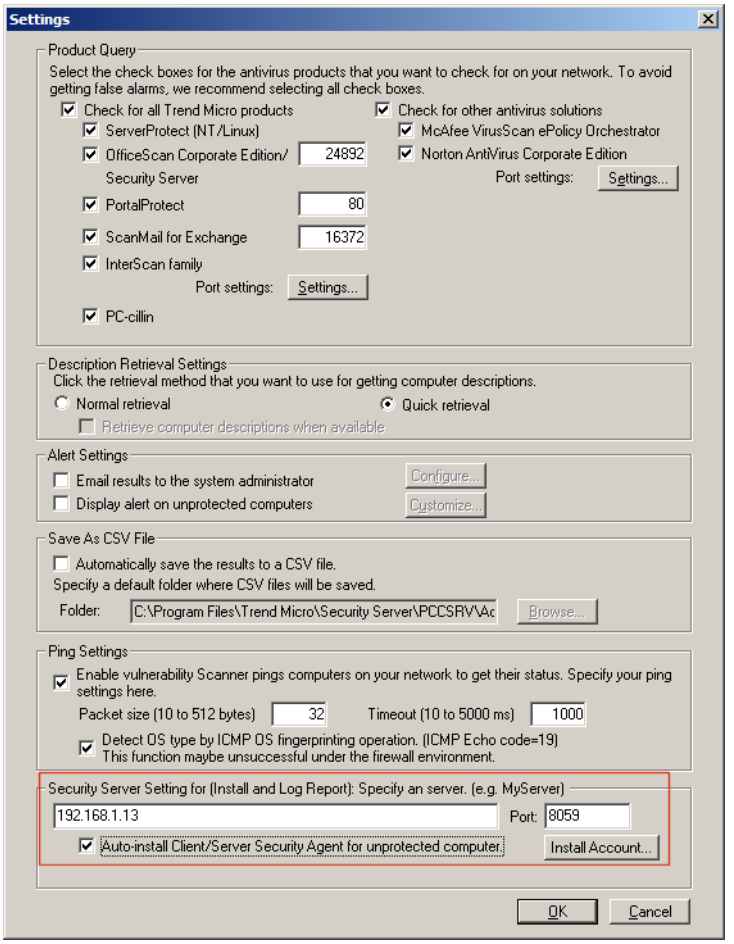


FIGURE 3-1. TMVS Settings screen

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** Client/Server 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 Client/Server Security Agent installation.

Installing MSA from the Web Console

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 Domain Administrator user name.
   - **Password.** The 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. Under **Spam Management Type**, select the spam management option. You can select either **End User Quarantine** or **Integrate with Outlook June E-mail Folder**.
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.
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 Client/Server Security Agent is properly installed.

To verify the installation:

- Look for the Worry-Free Business Security Advanced program shortcuts on the Windows **Start** menu of the Client running the Agent.
- Check if Worry-Free Business Security Advanced is in the **Add/Remove Programs** list of the Client's Control Panel.
- Use Vulnerability Scanner (see *Using Vulnerability Scanner to Verify the Client Installation* on page 3-17).
- Use the Client Mover tool (see *Client Mover* on page 14-11 or *Moving Clients* on page 4-9)

Using Vulnerability Scanner to Verify the Client Installation

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 Worry-Free Business Security Advanced online help.

Note: You can use Vulnerability Scanner on machines running Windows 2000 and 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 **Security Server** 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 yourself 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. Refer to *Choosing an Installation Method* on page 3-2.

Testing the Client Installation with the EICAR Test Script

Trend Micro recommends testing your product and confirming that it works by using the EICAR test script. EICAR, the European Institute for Computer Antivirus Research, developed the test script as a safe way to confirm that antivirus software is properly installed and configured. Visit the EICAR Web site for more information:

http://www.eicar.org

The EICAR test script is an inert text file with a `.com` extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software will react to

it as if it were a virus. Use it to simulate a virus incident and confirm that email notifications, HTTP scanning, and virus logs work properly.

WARNING! *Never use real virus/malware to test your antivirus installation.*

To test the Agent installation with the EICAR test script:

1. Make sure Real-time Scan is enabled on the Agent.
2. On the Client, copy the following string and paste it into Notepad or any plain text editor:

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

3. Save the file as `EICAR.com` to a temporary directory. Client/Server Security Agent should immediately detect the file.
4. To test other Clients on your network, attach the `EICAR.com` file to an email message and send it to one of the Clients.

Note: Trend Micro also recommends testing a compressed version of the EICAR file. Using compression software, compress the test script and perform the steps above.

To test the Agent installation HTTP scanning capability:

Download the EICAR.com test script from either of the following URLs:

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

Client/Server Security Agent should show that it detected the EICAR test file.

Removing Agents

There are two ways to remove Agents—from the Web console or by running its uninstallation program.

Removing Client/Server Security Agent Using Its Uninstallation Program

WARNING! *Removing Agents makes Clients vulnerable to threats.*

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** Client/Server Security Agent and click **Change/Remove**. The Client/Server Security Agent **Uninstallation** screen appears and prompts for the uninstall password, if configured.
3. Type the uninstall password and then click **OK**. **The** Client/Server Security Agent **Uninstallation** screen shows the progress of the uninstallation. When uninstallation is complete, the message "Uninstallation is complete" appears.

Removing the Client/Server Security Agent using the Web Console

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

WARNING! *Removing Agents makes Clients vulnerable to threats.*

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 Messaging Security Agent from Microsoft Exchange Servers

WARNING! *Removing Agents makes Clients vulnerable to threats.*

To remove Messaging Security Agent using the Web console:

1. On the Web console main menu, click **Security Settings**. The **Security Settings** screen appears.
2. Select the Microsoft Exchange server from which to uninstall Messaging Security Agent.
3. Click the **Remove** tool on the toolbar. The **Remove Computer** screen appears displaying the following options:
   - **Remove the selected inactive agent(s).** Select to remove the icon for Messaging Security Agent from the **Security Settings** screen.
   - **Uninstall the selected agent(s).** Select to completely uninstall Messaging Security Agent from the server and remove the icon from the **Security Settings** screen.
4. Click **Apply**. If necessary, type the account name and password for the Microsoft Exchange server from which you want to remove Messaging Security Agent.

   You will be prompted to verify your decision to uninstall Messaging Security Agent from the selected Exchange server.

5. Click **OK** to remove Messaging Security Agent from the selected Microsoft Exchange server.

Removing the Messaging Security Agent using its Uninstallation Program

WARNING! *Removing Agents makes Clients vulnerable to threats.*

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

Working with Groups

This chapter explains the concept and usage of groups in Worry-Free Business Security Advanced.

The topics discussed in this chapter include:

- *Overview of Groups* starting on page 4-2
- *Viewing Clients in a Group* starting on page 4-2
- *Adding Groups* starting on page 4-6
- *Removing Groups* starting on page 4-7
- *Adding Clients to Groups* starting on page 4-7
- *Moving Clients* starting on page 4-9
- *Replicating Group Settings* starting on page 4-10

Overview of Groups

In Worry-Free Business Security Advanced, groups are a collection of computers and servers (not Microsoft Exchange servers) that share the same configuration and run the same tasks. By grouping Clients, simultaneously configure, and manage, multiple Agents.

For ease of management, group Clients based on the departments to which they belong or the functions they perform. Also, group Clients that are at a greater risk of infection to apply a more secure configuration to all of them in just one setting. Refer to *Configuring Desktop and Server Groups* on page 5-1 for more information. Microsoft Exchange servers cannot be grouped together. To configure Microsoft Exchange servers, refer to *Configuring Microsoft Exchange Servers* on page 6-1.

By default, the Security Server creates groups based on your existing Windows Server domains and refers to each Client according to computer name. You can delete or rename the groups that the Security Server has created for you or transfer Clients from one group to another.

Viewing Clients in a Group

From the **Security Settings** screen, you can manage all Clients on which you installed Client/Server Security Agents and Messaging Security Agents and customize your security settings for agents.

Navigation Path: Security Settings > Select a Group

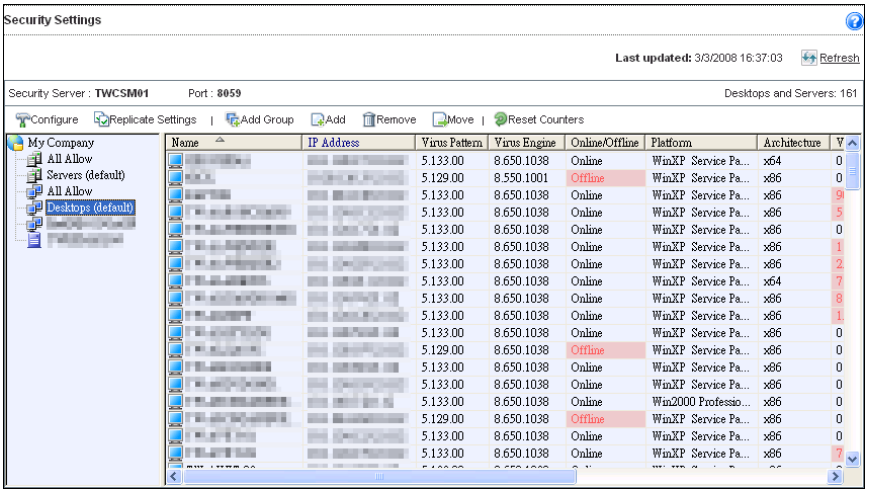


FIGURE 4-1. Security Settings screen showing Clients in a group

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: Microsoft Exchange servers with Messaging Security Agent installed are registered to the servers group. However, they are displayed individually in the Security Groups tree.

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. The Security Settings screen provides the following information about the Clients in a particular group:

- Name
- IP Address
- Online/Offline status
- Scheduled scan
- Manual scan
- Operating system
- Architecture
- Version of the virus engine and pattern
- Number of virus incidents detected
- Number of spyware incidents detected
- Number of violated URLs
- Number of spam incidents detected
- Status of the POP3 mail scan

Use this information 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

From here you can:

- **Configure groups:** Refer to *Configuring Desktop and Server Groups* on page 5-1 and *Configuring Microsoft Exchange Servers* on page 6-1.
- **Replicate settings from one group to another:** Refer to *Replicating Group Settings* on page 4-10.
- **Add new groups:** Refer to *Adding Groups* on page 4-6.
- **Remove groups:** Refer to *Removing Groups* on page 4-7.
- **Move Clients from one Group to another or one Security Server to another:** Refer to *Moving Clients* on page 4-9.

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

After an Upgrade

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

Worry-Free Business Security Advanced 5.1 does not support individual settings for a Client within a group. If your prior version contained these, they will now appear as a "mixed" group. To individually configure a Client, create a new group and add only this Client into the group. Configure the group as required.

Security Settings Toolbar

The Security Settings Toolbar contains the tools you need to work with Groups and Clients.

FIGURE 4-2. The Security Settings Toolbar

This section briefly describes the tools in the toolbar on the **Security Settings** screen. Refer to the online help for details about how to use these tools to configure your Client/Server Security Agents and Messaging Security Agents.

TABLE 4-1. Tools for Security Settings

Tool	Description
Configure	Configure Client settings at a group level for such settings as scanning, firewall, client privileges, and quarantine directory. Configure Anti-spam, Content Filtering, and Attachment Blocking for Microsoft Exchange servers. Refer to *Configuring Desktop and Server Groups* on page 5-1 and *Configuring Microsoft Exchange Servers* on page 6-1 for more details.
Replicate Settings	Use this tool to replicate configuration settings from one group of Clients to one or more other groups of Clients. Refer to *Replicating Group Settings* on page 4-10 for more details.
Add Group	Use this tool to create a new group of Clients. Refer to *Adding Groups* on page 4-6 for more details.

TABLE 4-1. Tools for Security Settings

Tool	Description
Add	Use Add to install Client/Server Security Agents, Messaging Security Agents, or add icons to Clients which already have an Agent. After adding a new Client, drag and drop the icon into an appropriate group.
Remove	Use this tool to either remove a Client or Group icon from the Web console or uninstall Client/Server Security Agent or Messaging Security Agent from the selected Client. Refer to *Removing Groups* starting on page 4-7 or *Removing Agents* starting on page 3-21.
Move	Use this tool to move a Client from one Security Server to another Security Server. Refer to *Moving Clients* on page 4-9 for more details.
Reset Counter	Resets the spam, virus/malware, spyware/grayware, and URL violation incidents.

Adding Groups

Create groups to collectively manage multiple Clients.

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

Navigation Path: Security Settings > Add Group

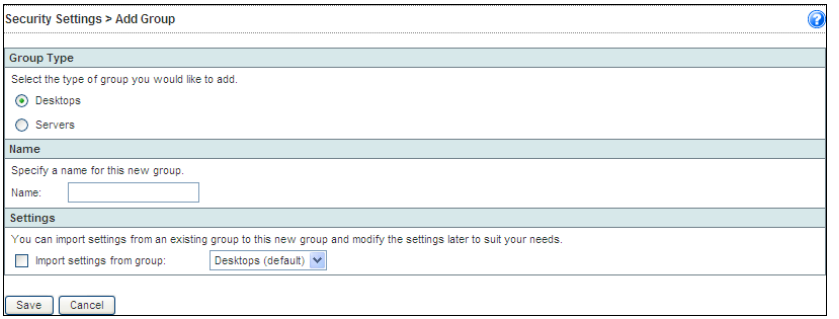


FIGURE 4-3. Add Group screen

To add a group:

1. From the **Add Group** screen, update the following as required:
   - **Group Type**
     - **Desktops**
     - **Servers**
   - **Name**
   - **Import settings from group:** Imports the security settings from the selected group.
2. Click **Save.**

Removing Groups

When Administrator's remove a group, all the Clients in the group re-register themselves with the Security Server and get included in the default Group, based on their operating system. For example, if the Client is a server, it gets included in the default server group.

Navigation Path: Security Settings

To remove a group:

1. From the **Security Settings** screen, select the Group.
2. Click **Remove.**

Adding Clients to Groups

In Worry-Free Business Security Advanced, add Clients to a Group using any one of the following methods:

- Email Notification Install
- Remote Install
- Create domain login script

Navigation Path: Security Settings

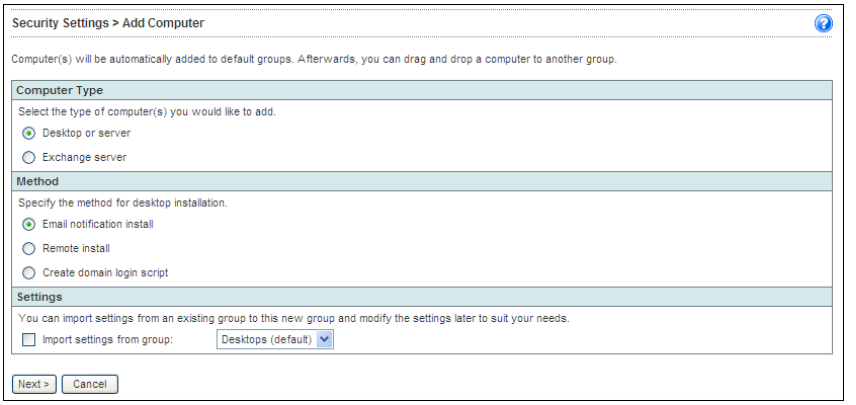


FIGURE 4-4. Add Computer screen

To add a Client to a Group:

1. From the **Security Settings** screen, click the **Add** tool on the toolbar.
2. Update the following as required:
   - **Computer Type:** The type of Client.
     - Desktop or server
     - Microsoft Exchange server
   - **Method**
     - **Remote install:** Remotely install the Agent on the Client. Refer to *Installing with Remote Install* on page 3-12 for more information.
     - **Create domain login script:** Install the Agent using domain login script. The next time the Client logs on to the network, the Agent will be installed. Refer to *Installing with Login Script Setup* on page 3-7 for more information.
   - **Microsoft Exchange Server Information**
     - **Server name:** Name or IP address of the target Microsoft Exchange server.
     - **Account:** Domain administrator account name.
     - **Password:** Domain administrator account password.

3. Click **Next**. Follow the onscreen instructions.

Tip: For more information about installing Agents, refer to *Installing Agents* on page 3-1.

Moving Clients

Worry-Free Business Security Advanced gives you the option to move Clients from one Group to another or one Security Server to another.

Navigation Path: Security Settings > Select a Group

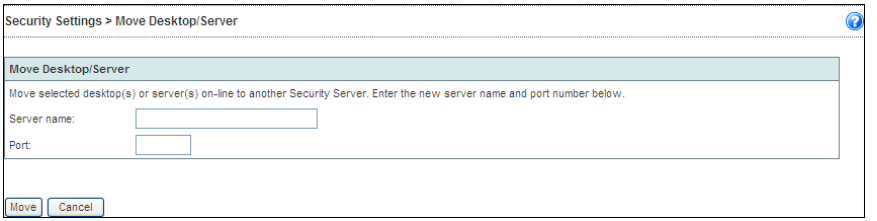


FIGURE 4-5. Move Desktop/Server screen

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.
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 > Select a Group

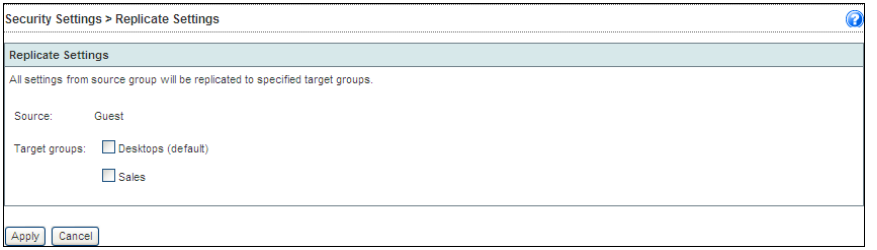


FIGURE 4-6. Replicate Settings screen

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**.

Chapter 5

Configuring Desktop and Server Groups

This chapter explains the steps necessary for configuring desktop and server groups. The topics discussed in this chapter include:

- *Overview of Configurable Options for Desktop and Server Groups* on page 5-2
- *Antivirus/Anti-spyware* on page 5-3
- *Firewall* on page 5-8
- *Web Threat Protection* on page 5-15
- *Behavior Monitoring* on page 5-16
- *TrendSecure* on page 5-21
- *POP3 Mail Scan* on page 5-23
- *Client Privileges* on page 5-25
- *Quarantine* on page 5-28

Overview of Configurable Options for Desktop and Server Groups

In Worry-Free Business Security Advanced, Groups are a collection of Clients that share the same configuration and run the same tasks. By grouping Clients, simultaneously configure, and manage, multiple Clients. For more information, refer to *Working with Groups* on page 4-1.

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	Enabled by Default?
Antivirus/Anti-spyware	Configure Real-time Scan, antivirus, and anti-spyware options	Enabled (Real-time Scan)
Firewall	Configure Firewall options	Disabled
Web Threat Protection	Configure In Office and Out of Office Web Threat Protection options	• In Office: Enabled, Low • Out of Office: Enabled, High
Behavior Monitoring	Configure Behavior Monitoring options	Disabled
TrendSecure	Configure In Office and Out of Office options for Transaction Protector and TrendProtect	• In Office: Disabled • Out of Office: Enabled
POP3 Mail Scan	Configure the scanning of POP3 email messages	Disabled
Client Privileges	Configure access to settings from the Client console	N/A
Quarantine	Specify the Quarantine directory	N/A

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

Antivirus/Anti-spyware

Virus/malware scanning is a central part of the Worry-Free Business Security Advanced strategy. During a scan, the Trend Micro scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus/malware contains a unique "signature" or string of tell-tale characters that distinguish it from any other code, the experts at TrendLabs capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When the scan engine detects file containing a threat, it executes an action such as clean, quarantine, delete, or replace with text/file. You can customize these actions when you set up your scanning tasks.

Worry-Free Business Security Advanced provides three types of scans to protect Clients from Internet threats:

- **Real-time Scan:** Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for threats. Refer to *Configuring Real-time Scan* on page 5-5 for more information. In the case of email messages, the Messaging Security Agent guards all known virus entry points with Real-time Scanning of all incoming messages, SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers. Refer to *Antivirus* on page 6-7.
- **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, Worry-Free Business Security Advanced takes actions against threats according to the actions set by the Administrator. Refer to *Manual Scan* on page 8-2 for more information.
- **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. Refer to *Scheduled Scan* on page 8-2 for more information.

Default Real-Time Scan Settings

By default, Worry-Free Business Security Advanced sets the Agents to run Real-time Scanning. No additional input is required to protect Clients.

Agents uses Trend Micro recommended settings when scanning for Internet threats. When it detects a threat, it performs the default action against those threats and logs the actions. View the results in the **Live Status** screen or by generating reports or log queries.

The default Real-Time Scan settings recommended by Trend Micro are:

- Real-time Scanning is enabled.
- Agents uses IntelliScan to decide which files to scan.
- Agents do not scan folders where Trend Micro products are installed.
- When Agents detect a threat, the default action is ActiveAction.
- When Agents detect spyware/grayware, the default action is to Clean. Agents delete uncleanable files.

Agents back up all files before taking action against detected threats.

TABLE 5-2. Recommended Actions for Threats

Threat	Recommended Action
All types	Clean
Virus/malware	Clean
Worms/Trojans	Quarantine
Joke	Quarantine
Packed files	Quarantine
Test virus	Pass
Other threats	Clean

Configuring Real-time Scan

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

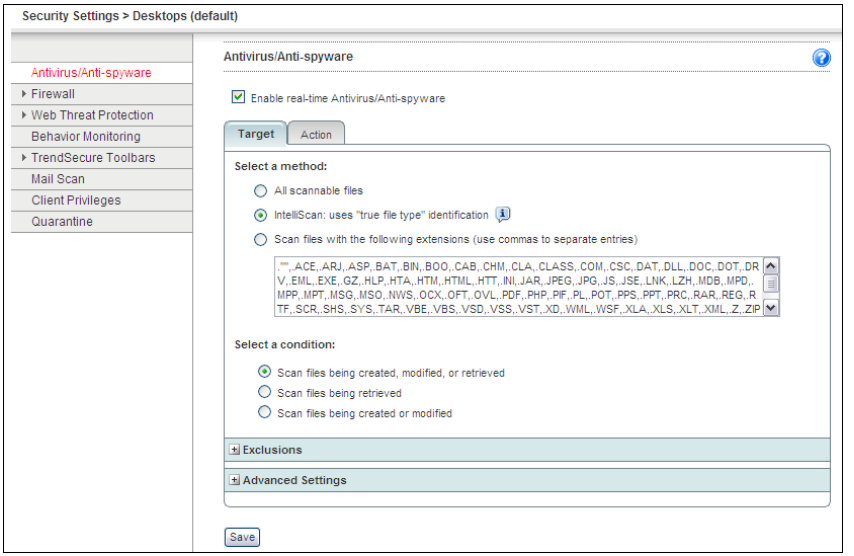


FIGURE 5-1. Security Settings > Antivirus/Anti-spyware screen

To configure Real-time Scan:

1. From the **Target** tab on the **Antivirus/Anti-spyware** screen, update the following as required:
   - **Enable real-time Antivirus/Anti-spyware**
   - Files to scan
     - **All scannable files:** Only encrypted or password-protected files are excluded.
     - **IntelliScan:** Scans files based on true-file type. Refer to *Trend Micro IntelliScan* on page C-4 for more information.
     - **Scan files with the following extensions:** Worry-Free Business Security Advanced will scan files with the selected extensions. Separate multiple entries with commas (,).

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

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

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

- **Spyware/Grayware Approved List** (for anti-spyware)**:** This list contains details of the approved spyware/grayware applications. Click the link to update the list. Refer to *Editing the Spyware/Grayware Approved List* on page 8-6 for more information.

2. From the **Action** tab on the **Antivirus/Anti-spyware** screen, specify how Worry-Free Business Security Advanced should handle detected threats:

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

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

   - **Action for Spyware/Grayware Detections**
     - **Clean:** When cleaning spyware/grayware, Worry-Free Business Security Advanced could delete related registry entries, files, cookies, and shortcuts. Processes related to the spyware/grayware could also be terminated.
     - **Deny Access**

   WARNING! *Denying spyware/grayware access to the Client does not remove the spyware/grayware threat from infected Clients.*

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

3. Click **Save.**

Additionally, configure who receives notifications when an event occurs. Refer to *About Notifications* on page 11-2.

Firewall

Help protect Clients from hacker attacks and network viruses by creating a barrier between the Client and the network. Firewall can block or allow certain types of network traffic. Additionally, Firewall will identify patterns in network packets that may indicate an attack on Clients.

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

Tip: Trend Micro recommends uninstalling other software-based firewalls before deploying and enabling Firewall.
For the latest information regarding third-party firewall compatibility issues, see http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-120437

Default Firewall Simple Mode Settings

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

Note: By default, WFBS-A disables the Firewall on all new Groups and Clients.

TABLE 5-3. Default Firewall Settings

Security Level	Description
Low	Inbound and outbound traffic allowed, only network viruses blocked.

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

Exception Name	Action	Direction	Protocol	Port
DNS	Allow	Incoming and outgoing	TCP/UDP	53
NetBIOS	Allow	Incoming and outgoing	TCP/UDP	137,138,139,445
HTTPS	Allow	Incoming and outgoing	TCP	443
HTTP	Allow	Incoming and outgoing	TCP	80
Telnet	Allow	Incoming and outgoing	TCP	23
SMTP	Allow	Incoming and outgoing	TCP	25
FTP	Allow	Incoming and outgoing	TCP	21
POP3	Allow	Incoming and outgoing	TCP	110
MSA	Allow	Incoming and outgoing	TCP	16372,16373

Location	Firewall Settings
In Office	Off
Out of Office	Off

Traffic Filtering

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

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

Refer to *Working with Firewall Exceptions* on page 5-13 to filter traffic.

Intrusion Detection System

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

- **Oversized Fragment:** This exploit contains extremely large fragments in the IP datagram. Some operating systems do not properly handle large fragments and may throw exceptions or behave in other undesirable ways.
- **Ping of Death:** A ping of death (abbreviated **"**POD**"**) is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer.
- **Conflicting ARP:** This occurs when the source and the destination IP address are identical.
- **SYN flood:** A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of `SYN` requests to a target's system.
- **Overlapping Fragment:** This exploit contains two fragments within the same IP datagram and have offsets that indicate they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle overlapping fragments and may throw exceptions or behave in other undesirable ways. This is the basis for the so called teardrop Denial of service Attacks.

- **Teardrop Attack:** The Teardrop attack involves sending IP fragments with overlapping, over-sized, payloads to the target machine. A bug in the TCP/IP fragmentation re-assembly code of various operating systems caused the fragments to be improperly handled, crashing them as a result of this.
- **Tiny Fragment Attack:** When any fragment other than the final fragment is less than 400 bytes, indicating that the fragment is likely intentionally crafted. Small fragments may be used in denial of service attacks or in an attempt to bypass security measures or detection.
- **Fragmented IGMP:** When a Client receives a fragmented Internet Group Management Protocol (IGMP) packet, the Client's performance may degrade or the computer may stop responding (hang) and require a reboot to restore functionality.
- **LAND Attack:** A LAND attack is a DoS (Denial of Service) attack that consists of sending a special poison spoofed packet to a computer, causing it to behave undesirably. The attack involves sending a spoofed `TCP SYN` packet (connection initiation) with the target host's IP address and an open port as both source and destination.

Stateful Inspection

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

Configuring the Firewall

Note: Configure the Firewall for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. Refer to *Location Awareness* on page 12-5.

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

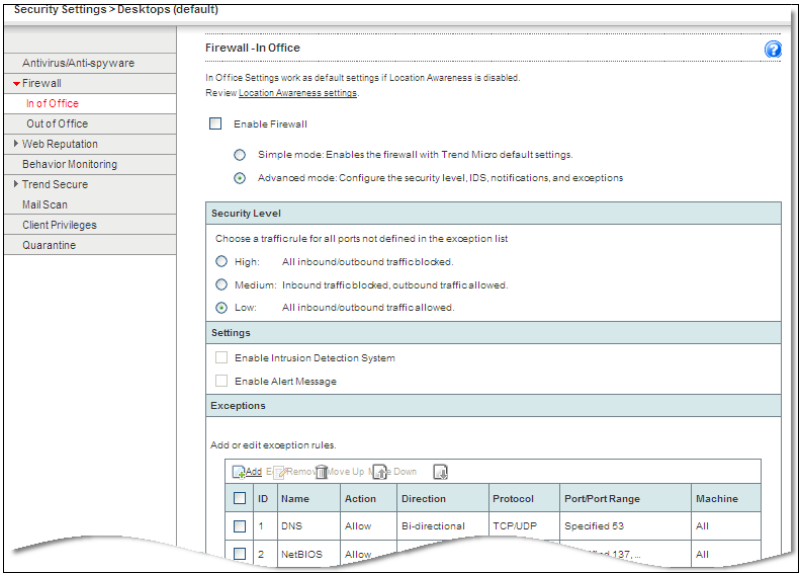


FIGURE 5-2. Firewall - In Office screen

To configure the Firewall:

1. From the **Firewall** screen, update the following options as required:
   - **Enable Firewall:** Select to enable the firewall for the group and location.
     - **Simple Mode:** Enables firewall with default settings. Refer to *Default Firewall Settings* on page 5-8.
     - **Advanced Mode:** Enables firewall with custom settings. Refer to *Advanced Firewall Options* on page 5-12 for configuration options.
2. Click **Save.** The changes take effect immediately.

Advanced Firewall Options

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

To configure advanced firewall options:

1. From the **Firewall** screen, select **Advanced Mode**.
2. Update the following options as required:
   - **Security Level:** The security level controls the traffic rules to be enforced for ports not in the exception list.
     - **High:** Blocks inbound and outbound traffic.
     - **Medium:** Blocks inbound traffic and allows outbound.
     - **Low:** Allows inbound and outbound traffic.
   - **Settings**
     - **Enable Intrusion Detection System:** Intrusion Detection System identifies patterns in network packets that may indicate an attack. Refer to *Intrusion Detection System* on page 5-10 for more information.
     - **Enable Alert Messages:** When Worry-Free Business Security Advanced detects a violation, the Administrator is notified. Refer to *Configuring Notifications* on page 14-12 for more information.
   - **Exceptions:** Ports in the exception list will not be blocked. Refer to *Working with Firewall Exceptions* **on page 5-13** for more information.
3. Click **Save**.

Working with Firewall Exceptions

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

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

Adding Exceptions

To add an exception:

1. From the **Firewall - Advanced Mode** screen in the **Exceptions** section, click **Add**.
2. Update the options as required:
   - **Name:** Specify a unique name for the exception.

- **Action: Block** or **Allow** the traffic for the selected protocol, ports, and Clients.
- **Direction: Inbound** refers to traffic flowing from the Internet and into your network. **Outbound** refers to traffic flowing from your network and into the Internet.
- **Protocol:** The network traffic protocol for this exclusion.
- **Ports**
  - **All ports** (default)
  - **Range**
  - **Specified ports:** Separate individual entries with commas.
- **Machine**
  - **All IP addresses** (default)
  - **IP range**
  - **Single IP:** The IP address of a particular Client.

3. Click **Save.** The **Firewall Configuration** screen appears with the new exception in the exception list.

Editing Exceptions

To edit an exception:

1. From the **Firewall - Advanced Mode** screen in the **Exceptions** section, select the exclusion you want to edit.
2. Click **Edit.**
3. Update the options as required. Refer to *Adding Exceptions* on page 5-13 for more information.
4. Click **Save.**

Removing Exceptions

To remove an exception:

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

Web Threat Protection

Web Threat Protection 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 Threat Protection blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list. For information on adding a URL to the Approved URL list, refer to *Web Threat Protection* on page 12-7 for more details.

Configuring Web Threat Protection

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

Note: Configure the Web Threat Protection settings for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. Refer to *Location Awareness* on page 12-5.

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

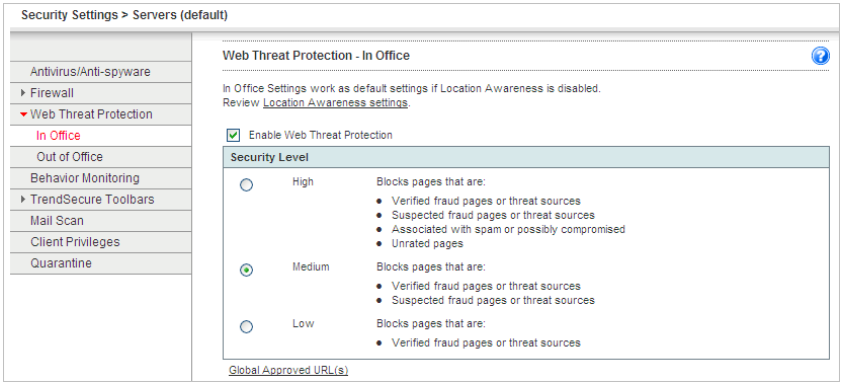


FIGURE 5-3. Security Settings > Web Threat Protection screen

To edit Web Threat Protection settings:

1. From the **Web Threat Protection** screen, update the following as required:
   - **Enable Web Threat Protection**
   - **Security Level**
     - **High:** Blocks pages that are:
       - Verified fraud pages or threat sources
       - Suspected fraud pages or threat sources
       - Associated with spam or possibly compromised
       - Unrated pages
     - **Medium:** Blocks pages that are:
       - Verified fraud pages or threat sources
       - Suspected fraud pages or threat sources
     - **Low:** Blocks pages that are verified fraud pages or threat sources
2. 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. To troubleshoot the validity of digital signatures, refer to *Invalid/Expired Digital Signatures* on page 15-17.

Refer to Table 5-4 on page 5-16 to view the description and default value of the monitored changes.

TABLE 5-4. Description and Default Values of Monitored Changes

Monitored Change	Description	Default Value
New Startup Program	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.	Ask when necessary

TABLE 5-4. Description and Default Values of Monitored Changes

Monitored Change	Description	Default Value
Hosts File Modification	The Hosts file matches domain names with IP addresses. Many malicious programs modify the Hosts file so that the Web browser is redirected to infected, non-existent, or fake Web sites.	Always block
Program Library Injection	Many malicious programs configure Windows so that all applications automatically load a program library (DLL). This allows the malicious routines in the DLL to run every time an application starts.	Ask when necessary
New Internet Explorer Plugin	Spyware/grayware programs often install unwanted Internet Explorer plugins, including toolbars and Browser Helper Objects.	Ask when necessary
Internet Explorer Setting Modification	Many virus/malware change Internet Explorer settings, including the home page, trusted Web sites, proxy server settings, and menu extensions.	Always block
Shell Modification	Many malicious programs modify Windows shell settings to associate themselves to certain file types. This routine allows malicious programs to launch automatically if users open the associated files in Windows Explorer. Changes to Windows shell settings can also allow malicious programs to track the programs used and start alongside legitimate applications.	Ask when necessary
New Service	Windows services are processes that have special functions and typically run continuously in the background with full administrative access. Malicious programs sometimes install themselves as services to stay hidden.	Ask when necessary
Security Policy Modification	Modifications in Windows Security Policy can allow unwanted applications to run and change system settings.	Always block
Firewall Policy Modification	The Windows Firewall policy determines the applications that have access to the network, the ports that are open for communication, and the IP addresses that can communicate with the computer. Many malicious programs modify the policy to allow themselves to access to the network and the Internet.	Ask when necessary
System File Modification	Certain Windows system files determine system behavior, including startup programs and screen saver settings. Many malicious programs modify system files to launch automatically at startup and control system behavior.	Always block

TABLE 5-4. Description and Default Values of Monitored Changes

Monitored Change	Description	Default Value
Duplicated System File	Many malicious programs create copies of themselves or other malicious programs using file names used by Windows system files. This is typically done to override or replace system files, avoid detection, or discourage users from deleting the malicious files.	Ask when necessary
Layered Service Provider	A Layered Service Provider (LSP) can manipulate inbound and outbound network traffic. Malicious programs can use LSPs to intercept network communication and gain network access.	Ask when necessary

Environment Variables

Worry-Free Business Security Advanced supports using environment variables to specify specific folders on the Client. Use these variables to create exceptions for specific folders. The following table describe the available variables:

TABLE 5-5. Supported Variables

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

Configuring Behavior Monitoring

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

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

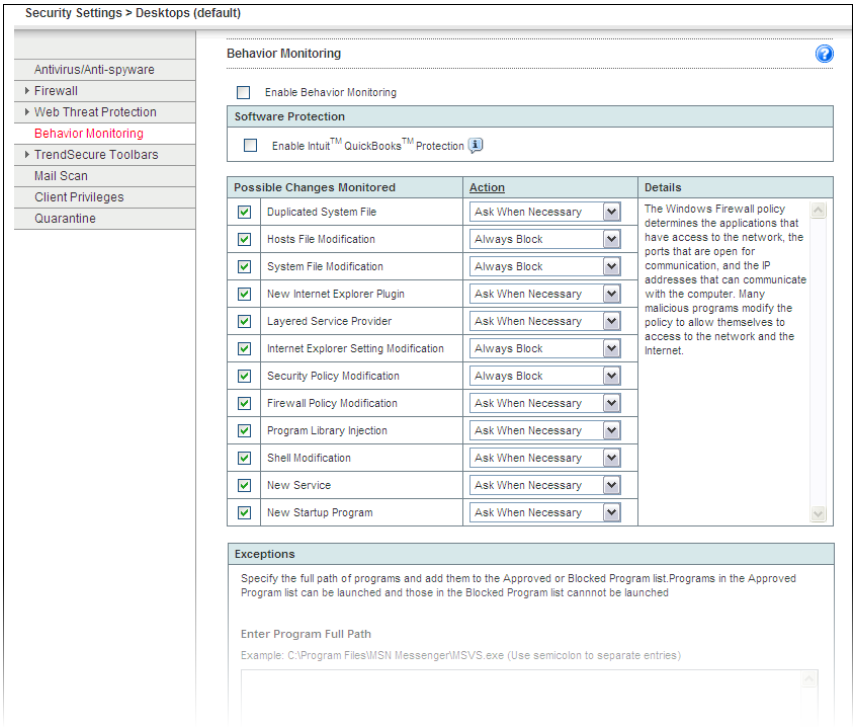


FIGURE 5-4. Behavior Monitoring screen

To edit Behavior Monitoring settings:

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

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

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

  The following products are supported:

  - QuickBooks Simple Start
  - QuickBooks Pro
  - QuickBooks Premier
  - QuickBooks Online

Tip: Trend Micro recommends enabling this feature.

- **Monitored Changes:** Select **Always Allow**, **Ask When Necessary**, or **Always Block** for each monitored change. Refer to Table 5-4 on page 5-16 for information on the different changes.
- **Exceptions:** Exceptions include an **Approved Program List** and a **Blocked Program List**: Programs in the **Approved Programs List** can be started even if it violates a monitored change, while programs in the **Blocked Program List** can never be started.
  - **Full Path of Program:** Type the full path of the program. Separate multiple entries with semicolons (;). Click **Add to Approved Programs List** or **Add to Blocked Programs List**. Use environment variables to specify paths, if required. Refer to Table 5-5, "Supported Variables," on page 5-18 for the list of supported variables.
  - **Approved Programs List:** Programs (maximum of 100) in this list can be started. Click the corresponding  icon to delete an entry.
  - **Blocked Programs List:** Programs (maximum of 100) in this list can never be started. Click the corresponding  icon to delete an entry.

2. Click **Save.**

TrendSecure

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

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

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

Note: Configure the TrendSecure settings for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. Refer to *Location Awareness* on page 12-5.

Configuring TrendSecure

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

Note: Configure TrendSecure for In Office and Out of Office Connections. If Location Awareness is disabled, Internal Connection settings will be enforced for Out of Office connections. Refer to *Location Awareness* on page 12-5.

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

To edit the availability of TrendSecure tools:

1. From the **TrendSecure In Office/Out of Office** screen, update the following as required:
   - **Enable Wi-Fi Advisor:** Checks the safety of wireless networks based on the validity of their SSIDs, authentication methods, and encryption requirements.
   - **Enable Page Ratings:** Determines the safety of the current page.

2. Click **Save.**

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

POP3 Mail Scan

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

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

POP3 Mail Scan Requirements

POP3 Mail Scan supports the following mail clients:

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

Anti-Spam Toolbar Requirements

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

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

The Anti-Spam toolbar supports the following operating systems:

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

Enabling Mail Scan

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

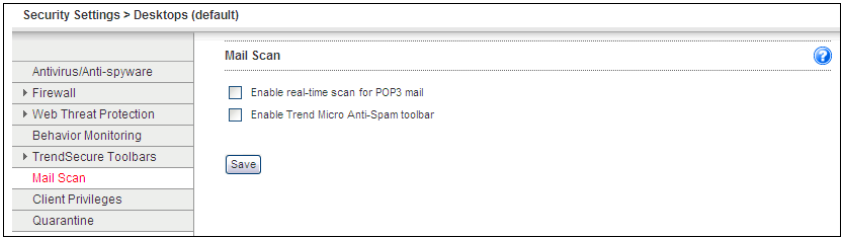


FIGURE 5-5. Mail Scan screen

To edit the availability of Mail Scan:

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

Configuring POP3 Mail Scan to Scan Other Ports

POP3 Mail Scan can be configured to scan messages sent through ports other than default port 110.

Note: This *advanced* procedure will require you to modify the Windows registry and restart the Trend Micro proxy service on individual clients. Perform this procedure only when necessary and ensure that you back up the registry before you begin.

To configure POP3 Mail Scan to scan non-default ports:

1. Click **Start > Run**.
2. Type **REGEDIT** and click **OK**. Registry Editor opens.
3. Navigate to the following registry subkey:

```
HKEY_LOCAL_MACHINE\Software\TrendMicro\NSC\TmProxy\
ProtocolHandler\pop3\Redirect\Pop3Mailer
```

4. Right click the value named **Port** and select **Modify**.
5. Ensure that **Decimal** is selected as the **Base** and then specify the port number that you want scanned under **Value data**.
6. Click **OK** and then close Registry Editor.
7. Click **Start > Run**.
8. Type **CMD** and click **OK**.
9. In the command prompt, enter the command **net stop tmproxy** to stop the Trend Micro proxy service
10. After the service stops, enter the command **net start tmproxy** to start the proxy service.

Client Privileges

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

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

Configuring Client Privileges

Navigation Path: Security Settings > Select a group **> Configure > Client Privileges**

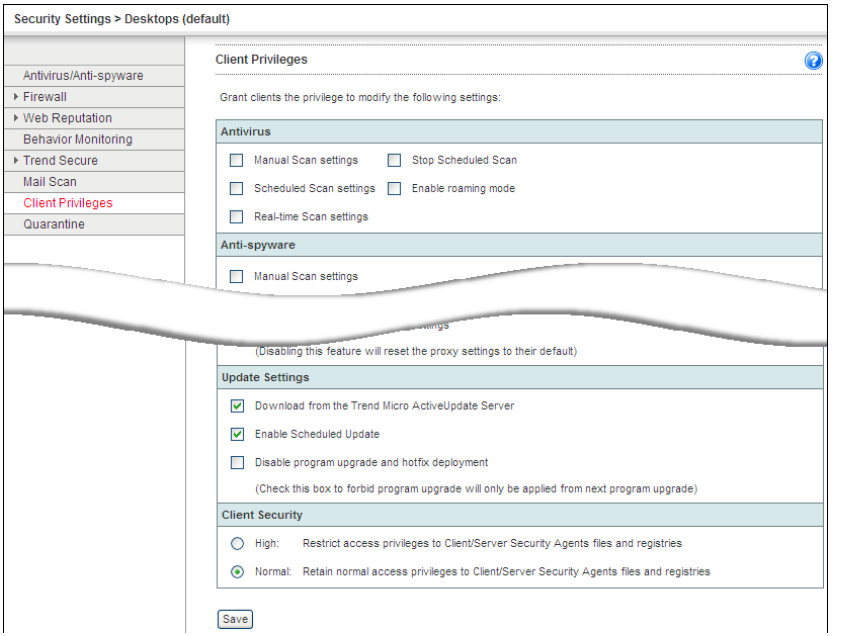


FIGURE 5-6. Client Privileges screen

To grant privileges to Clients:

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

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

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

- **Web Threat Protection**
  - **Edit approved URL list**
- **Behavior Monitoring**
  - **Display Behavior Monitoring tab and allow users to customize the lists:** Allow users to enable/disable Behavior Monitoring and configure the Exception List and the Software Protection List.
- **Mail Scan**
  - **Allow users to configure real-time scan for POP3 mail**
- **Proxy Setting**
  - **Allow users to configure proxy settings**
- **Update Privileges**
  - **Perform "Update Now"**
  - **Enable/Disable Scheduled Update**
- **Update Settings**
  - **Download from Trend Micro ActiveUpdate Server:** When users initiate an update, the Agent gets updates from the update source specified on the **Update Source** screen. If the update fails, the Agents attempt to update from the Security Server. Selecting **Download from the Trend Micro ActiveUpdate Server** enables Agents to attempt to update from the Trend Micro ActiveUpdate Server if the update from the Security Server fails.

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

  - **Enable Scheduled Update**
  - **Disable program upgrade and hot fix deployment**
- **Client Security**
  - **High:** Prevents access to Agent folders, files, and registry entries.
  - **Normal:** Provides read/write access to Agent folders, files, and registry entries.

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

---

2. Click **Save**.

Quarantine

The Quarantine directory stores the infected files. The quarantine directory can reside on the Client itself or on another server. If an invalid quarantine directory is specified, Agents uses the default quarantine directory on the Client:

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

The default folder on the server is:

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

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

Configuring the Quarantine Directory

Navigation Path: Security Settings > Select a group **> Configure > Quarantine**

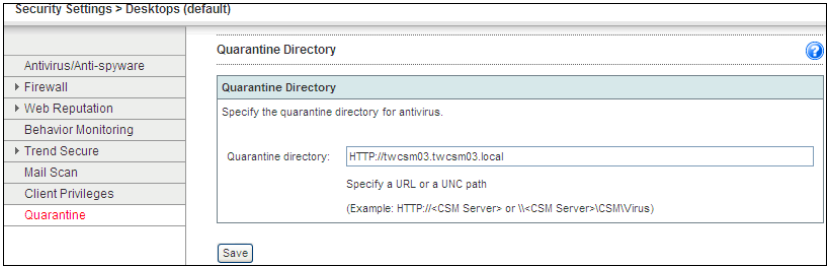


FIGURE 5-7. Quarantine Directory screen

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

Configuring Microsoft Exchange Servers

This chapter describes the Messaging Security Agent and explains how to set Real-time Scan options, configure anti-spam, content filtering, attachment blocking, and quarantine maintenance options for Microsoft Exchange™ servers.

The topics discussed in this chapter include:

- *About Messaging Security Agents* on page 6-2
- *Antivirus* on page 6-7
- *Anti-Spam* on page 6-12
- *Content Filtering* on page 6-20
- *Attachment Blocking* on page 6-35
- *Quarantine* on page 6-40
- *Operations* on page 6-49

About Messaging Security Agents

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

- reduce spam
- block email messages based on content
- block or restrict email messages with attachments

Messaging Security Agents can only be installed on Microsoft Exchange servers. The Groups 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.

Worry-Free Business Security Advanced 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 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)

MSA 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 6-1. 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 *clean* for virus/malware. Under some conditions, the Messaging Security Agent cannot clean a file. See *Uncleanable Files* on page 6-4. 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.

TABLE 6-1. Messaging Security Agent Customized Actions

Action	Description
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 *Quarantine Directories* on page 6-41 for more information about the quarantine folder.
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. **Note:** Excluded, encrypted, or password-protected files are delivered to the recipient without updating the logs.

Uncleanable Files

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/malware 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

Notifications for Detected Threats

When the Messaging Security Agent (MSA) detects a threat in an email, it can send notifications to the email sender and/or recipients. From the **Action** tab area of the Antivirus/Anti-spyware screen, you can configure MSA to send notifications to all senders and/or recipients or to just internal senders and/or recipients. You can also configure MSA to not send notifications when it detects spoofing mails.

Advanced Macro Scanning

The Messaging Security Agent uses the virus pattern file to identify known malicious macro codes during regular scanning. The Messaging Security Agent takes action against malicious macro code depending on the action that you configure from the Antivirus screen. Use Advanced macro scanning to gain additional protection against malicious macro code.

Advanced macro scanning supplements regular virus/malware scanning. It uses heuristic scanning to detect macro viruses or simply strips all detected macro code. 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 a malicious macro code is detected using heuristic scanning, the Messaging Security Agent 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 Messaging Security Agent strips all macro code from the scanned files.

Configurable Options for Microsoft Exchange Server Groups

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

- **Antivirus:** Configure Real-time Scan options for the Microsoft Exchange server.
- **Anti-spam:** Set spam detection level, configure Approved/Blocked Senders list, and set actions for spam.
- **Content Filtering:** Enable and configure content filtering.
- **Attachment Blocking:** Specify attachment blocking requirements.
- **Quarantine:** Perform queries, quarantine maintenance, and set Quarantine directories.
- **Operations:** Perform spam maintenance, set internal email address, and set system debugger options.

Default Messaging Security Agent Settings

Consider the options listed in Table 6-2 on page 6-6 to help you optimize your Messaging Security Agent configurations.

TABLE 6-2. 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 End User Quarantine installed)	Not applicable
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

TABLE 6-2. Trend Micro Default Actions for the Messaging Security Agent

Scan option	Real-time Scan	Manual and Scheduled Scan
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)
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)

Antivirus

Worry-Free Business Security Advanced 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 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, Worry-Free Business Security Advanced takes actions against threats according to the actions set by the Administrator. Refer to *Manual Scan* on page 8-2 for more information.
- **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. Refer to *Scheduled Scan* on page 8-2 for more information.

Configuring Real-time Scan for Messaging Security Agents

Configure Messaging Security Agents to scan specific targets and set actions to take when it discovers a security threat in the targeted messages and files. Also, configure Agents to send notifications when it takes actions against security risks. Refer to Table 6-2 on page 6-6 for the default settings.

Navigation Path: Security Settings > Select a Microsoft Exchange Server > **Configure > Antivirus**

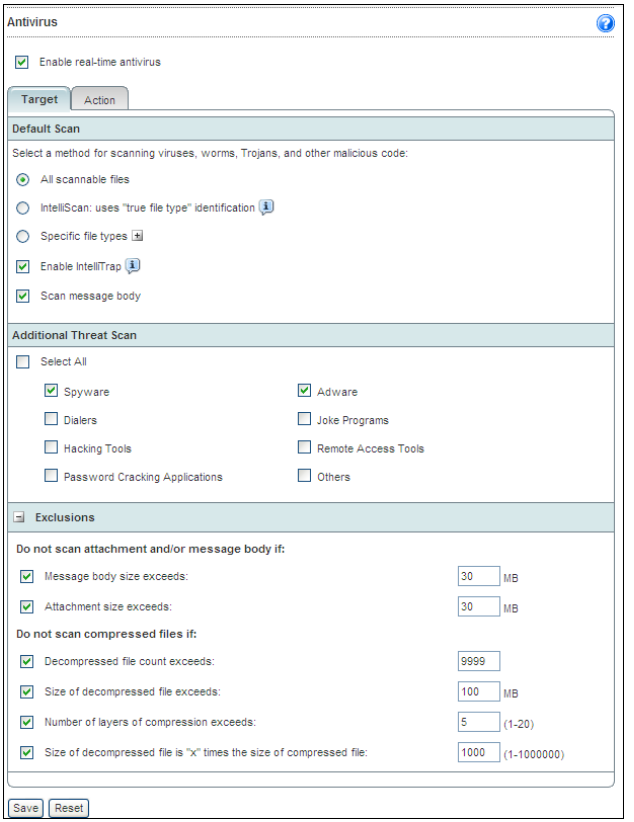


FIGURE 6-1. Security Settings > Antivirus screen

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**

WARNING! *Disabling Real-time Scan makes the Microsoft Exchange server vulnerable to infection.*

- Files to scan
  - **IntelliScan:** Scans files based on true-file type. Refer to *Trend Micro IntelliScan* on page C-4 for more information.
  - **All scannable files:** Only encrypted or password-protected files are excluded.
  - **Specific file types:** Worry-Free Business Security Advanced will scan files with the selected extensions. Separate multiple entries with commas (,).
  - **Enable IntelliTrap:** IntelliTrap detects malicious code such as bots in compressed files. Refer to *Trend Micro IntelliTrap* on page C-6 for more information.
  - **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. Refer to *Glossary of Terms* **on page F-1** 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. Refer to *Trend Micro ActiveAction* on page C-4 for more information.

- **Perform the same action for all detected Internet threats:** Select from Clean, Replace with Text/File, Delete Entire message, Pass, or Quarantine message part. Refer to Table 6-1 on page 6-3 for more information.
- **Specify action per detected threats:** Select from Clean, Replace with Text/File, Delete Entire message, Pass, Quarantine entire message, or Quarantine message part for each type of threat. Refer to Table 6-1 on page 6-3 for more information.
- **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. Refer to Table 6-1 on page 6-3 for more information.
- Set the secondary action for unsuccessful cleaning attempts. Select from Replace with Text/File, Delete Entire message, Pass, or Quarantine message part.
- **Backup infected file before cleaning:** 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.

- **Notifications:** Worry-Free Business Security Advanced 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.
  - **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:** Refer to *Advanced Macro Scanning* on page 6-5 for more information.
  - **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.**

   Additionally, configure who receives notifications when an event occurs. Refer to *About Notifications* on page 11-2.

Anti-Spam

Worry-Free Business Security Advanced provides two ways to combat spam — Email Reputation and Content Scanning.

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 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.

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.

Content Scanning

Content Scanning determines 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.

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 mark(!!!!) 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 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.

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

- Quarantines spam messages to a server-side spam folder
- Quarantines spam messages to user's spam folder
- Deletes the spam message
- Tags and delivers messages as spam

Note: Microsoft Outlook may automatically filter and send messages that 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 Web site. Here the user is asked to update personal information such as passwords, social security numbers, and credit card numbers in an attempt to trick a recipient into providing private information that will be used for identity theft.

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

- **Quarantine message to server-side spam folder:** The **Messaging Security Agent** sends the entire message to the Security Server for quarantine.
- **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.

Approved and Blocked Senders Lists

An Approved Senders list is a list of trusted email addresses. The Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent detects them as spam and takes action against them. If the Messaging Security Agent 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 Messaging Security Agent 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).

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

The Messaging Security Agent does not support the wildcard match on the user name part. However, if you type a pattern such as "*@trend.com", the Messaging Security Agent 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 6-3. 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 6-3. Email Address Matches for Wildcards

Pattern	Matched samples	Unmatched samples
..*.example.com *****.example.com	The same as "*.example.com"	
example.com example.com example.*.com @*.example.com	Invalid patterns	

Configuring 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.

Navigation Path: Security Settings > Select a Microsoft Exchange Server > **Configure > Anti-Spam > Email Reputation**

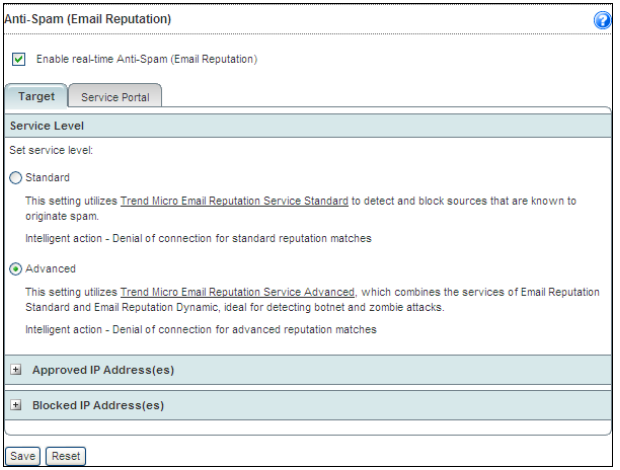


FIGURE 6-2. Email Reputation screen

To configure Email Reputation:

1. From the **Target** tab on the **Email Reputation** screen, update the following as required:
   - **Enable real-time Anti-Spam (Email Reputation)**
   - **Service Level:** Refer to *Email Reputation* on page 6-12 for information about the available services.
     - **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:

   https://nrs.nssg.trendmicro.com/index.php

   to view reports. Refer to Email Reputation documentation for more information.

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

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 Worry-Free Business Security Advanced detects spam.

Navigation Path: Security Settings > Select a Microsoft Exchange Server > **Configure > Anti-Spam > Content Scanning**

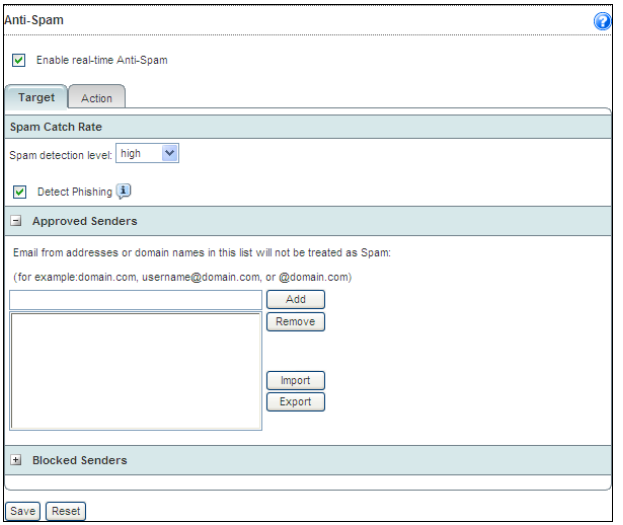


FIGURE 6-3. Content Scanning screen

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:** Refer to *Spam Detection* on page 6-13 for information about the available services.
   - **Detect Phishing:** Phishing incidents encourage users to click a link that will redirect their browser to a fraudulent Web site that imitates an authentic Web site. Refer to *Phishing* on page 6-14 for information.
   - **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**. Refer to *Approved and Blocked Senders Lists* **on page 6-15** for information

- **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.** Refer to *Approved and Blocked Senders Lists* on page 6-15 for information

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

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.

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.

Keywords

In Worry-Free Business Security Advanced, 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

Worry-Free Business Security Advanced 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 6-4. Using Operators

Operator	How it works	Example
any keyword	MSA searches content that matches the word	Type the word and add it to the keyword list
OR	MSA searches for any of the keywords separated by OR For example, apple OR orange. 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"
AND	MSA searches for all of the keywords separated by AND For example, apple AND orange. 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	MSA excludes keywords following NOT from search. For example, .NOT. juice. 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: 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 6-4. Using Operators

Operator	How it works	Example
REG	To specify a *regular expression*, add a .REG. operator before that pattern (for example, .REG. a.*e). Refer to *Regular Expressions* on page 6-24 for more information,	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

MSA offers simple and powerful features to create highly specific filters. Consider the following, when creating your Content Filtering rules:

- By default, MSA searches for exact matches of keywords. Use *regular expressions* to set MSA to search for partial matches of keywords. For more information, refer to *Regular Expressions* on page 6-24.
- 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 6-5 for more information about using keywords on multiple lines.
- You can also set MSA to search for synonyms of the actual keywords.

TABLE 6-5. 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."
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 6-5. How to Use Keywords

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 Web sites 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's recommendation is to start with simple regular expressions that do not use complex syntax. When introducing new rules, use the archive action and observe how 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 6-6. 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
?	The question mark character means zero or one instances of the preceding element.	do**?**g matches dg or dog but not doog, dooog, etc.
( )	Parenthesis characters group whatever is between them to be considered as a single entity.	d**(**eer**)+** matches deer or deereer or deereereer, etc. The + sign is applied to the substring within parentheses, so the regex looks for d followed by one or more of the grouping "eer."

TABLE 6-6. Counting and Grouping

Element	What it means	Example
[ ]	Square bracket characters indicate a set or a range of characters.	d**[**aeiouy**]+** matches da, de, di, do, du, dy, daa, dae, dai, etc. The + sign is applied to the set within brackets parentheses, so the regex looks for d followed by one or more of any of the characters in the set [aeioy]. d[A-Z] matches dA, dB, dC, and so on up to dZ. The set in square brackets represents the range of all upper-case letters between A and Z.
[^]	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.	d[^aeiouy] matches db, dc or dd, d9, d#--d followed by any single character except a vowel.
{ }	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 6-7. 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.

TABLE 6-7. Character Classes (shorthand)

Element	What it means	Example
\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.
\s	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [[:space]]	vegetable**s** 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 [^[:space]]	vegetable**\S** 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 6-8. Character Classes

Element	What it means	Example
[:alpha:]	Any alphabetic characters	.REG. [[:alpha:]] matches abc, def, xxx, but not 123 or @#$.
[:digit:]	Any digit character; functionally equivalent to \d	.REG. [[:digit:]] matches 1, 12, 123, etc.
[:alnum:]	Any “word” character--that is, any alphanumeric character; functionally equivalent to \w	.REG. [[:alnum:]] matches abc, 123, but not ~!@.

TABLE 6-8. Character Classes

Element	What it means	Example
[:space:]	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to \s	.REG. (vegetable)[[:space:]] 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.
[:graph:]	Any characters except space, control characters or the like	.REG. [[:graph:]] matches 123, abc, xxx, ><", but not space or control characters.
[:print:]	Any characters (similar with [:graph:]) but includes the space character	.REG. [[:print:]] matches 123, abc, xxx, ><", and space characters.
[:cntrl:]	Any control characters (e.g. CTRL + C, CTRL + X)	.REG. [[:cntrl:]] matches 0x03, 0x08, but not abc, 123, !@#.
[:blank:]	Space and tab characters	.REG. [[:blank:]] matches space and tab characters, but not 123, abc, !@#
[:punct:]	Punctuation characters	.REG. [[:punct:]] matches ; : ? ! ~ @ # $ % & * ' " , etc., but not 123, abc
[:lower:]	Any lowercase alphabetic characters (Note: 'Enable case sensitive matching' must be enabled or else it will function as [:alnum:])	.REG. [[:lower:]] matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, !@#.
[:upper:]	Any uppercase alphabetic characters (Note: 'Enable case sensitive matching' must be enabled or else it will function as [:alnum:])	.REG. [[:upper:]] matches ABC, DEF, STRESS, DO, etc., but not abc, Def, Stress, Do, 123, !@#.
[:xdigit:]	Digits allowed in a hexadecimal number (0-9a-fA-F)	.REG. [[:xdigit:]] matches 0a, 7E, 0f, etc.

TABLE 6-9. 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 6-10. 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.
\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.

TABLE 6-10. Escape Sequences and Literal Strings

Element	What it means	Example
\r	Indicates a carriage return character.	(stress)**\r** matches any block of text that contained the sub-string "stress" followed immedi-ately 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 sub-string "stress" followed immedi-ately 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
\xhh	Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).	**\x**7E(\w){6} matches any block of text containing a "word" of exactly six alphanumeric char-acters 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. Refer to *Keywords* on page 6-21 for more information.

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 6-11. Numbers matching the Social Security Regular Expression

.REG. \b\d{3}-\d{2}-\d{4}\b	
333-22-4444	Match
333224444	Not a match
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
```

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.

Viewing Content Filtering Rules

The Messaging Security Agent (MSA) displays all the content filtering rules on the Content Filtering screen.

Navigation Path: Security Settings > Select a Microsoft Exchange Server **> Configure > Content Filtering**

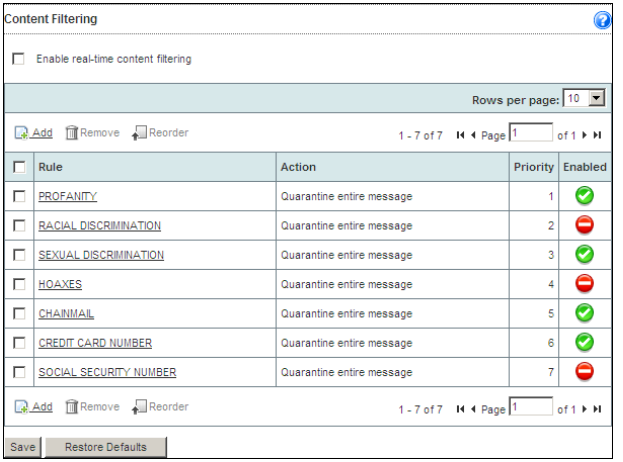


FIGURE 6-4. Content Filtering screen

This screen shows summary information about the rules including:

- **Rule**

- **Action:** MSA takes this action when it detects undesirable content.
- **Priority:** 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:** Refer to *Adding/Editing Content Filtering Rules* on page 6-33.
- **Reorder rules:** Refer to *Reordering Rules* on page 6-35.
- **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**.

Adding/Editing Content Filtering Rules

To create a content filtering rule, you move through a series of steps. 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.

Navigation Path: Security Settings > Select a Microsoft Exchange Server **> Configure > Content Filtering > Add/Edit a Rule**

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**.

   - **Filter messages that match any condition defined**

     i. Name the rule.

     ii. Set the scan conditions.

     iii. Add the keywords. Include synonyms and/or case-sensitive criteria.

     iv. 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.

   - **Filter messages that match all conditions defined**

     i. Name the rule.

     ii. Set the scan conditions.

     iii. 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.

   - **Monitor the message content of particular email accounts**

     i. Name the rule.

     ii. Set the accounts to monitor.

     iii. Set the scan conditions.

     iv. Add the keywords. Include synonyms and/or case-sensitive criteria.

     v. 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.

   - **Create an exception list for email accounts**

     i. Name the rule.

     ii. Set the accounts to exclude.

Note: Messaging Security Agent does not apply content rules with a lower priority than this rule to email accounts in this list.

3. Click **Finish.**

Reordering Rules

MSA 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. 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 > Select a Microsoft Exchange Server **> 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.

Attachment Blocking

Attachment blocking prevents attachments in email messages being delivered to the Microsoft Exchange Information Store. Configure the Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent will detect attachment types according to their name.
- **Attachment type:** The Messaging Security Agent examines the file header rather than the file name to ascertain the actual file type.

Attachment Blocking Actions

You can configure the Messaging Security Agent to take action against email messages containing detected threats. The following table lists the actions the Messaging Security Agent can take.

TABLE 6-12. Attachment Blocking Actions

Action	Description
Replace with text/file	The Messaging Security Agent 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 Messaging Security Agent deletes the entire email message.

Configuring Attachment Blocking

Configure the attachments to block and specify the action for blocked messages.

Navigation Path: Security Settings > Select a Microsoft Exchange Server > **Configure > Attachment Blocking**

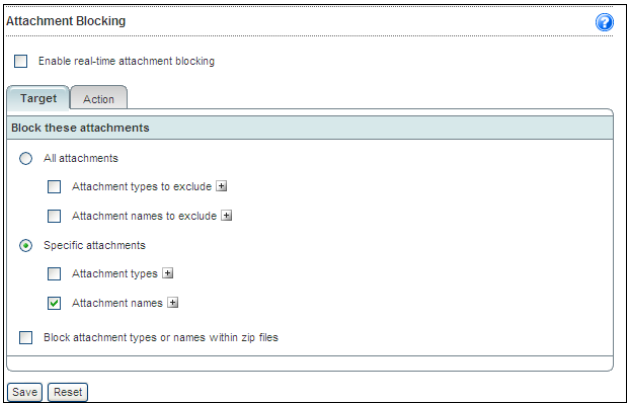


FIGURE 6-5. Attachment Blocking screen

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:** Refer to Table 6-12 on page 6-38 for information.
   - **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, Worry-Free Business Security Advanced will replace the threat with this text string and file.

3. Click **Save.**

Quarantine

When Messaging Security Agents detect a threat, spam, restricted attachments 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. For more information on restoring files encrypted by MSA, refer to *Restore Encrypted Virus* on page 14-8.

Administrators can query the quarantine database to gather information about quarantined messages. See *Querying Quarantine Directories* on page 6-43.

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 Messaging Security Agent 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 Messaging Security Agent quarantines email messages according to configured actions. Create one quarantine folder for each action. There are four quarantine directories in Worry-Free Business Security Advanced, they are:

- **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 > Select a Microsoft Exchange Server > **Configure > Quarantine > Directory**

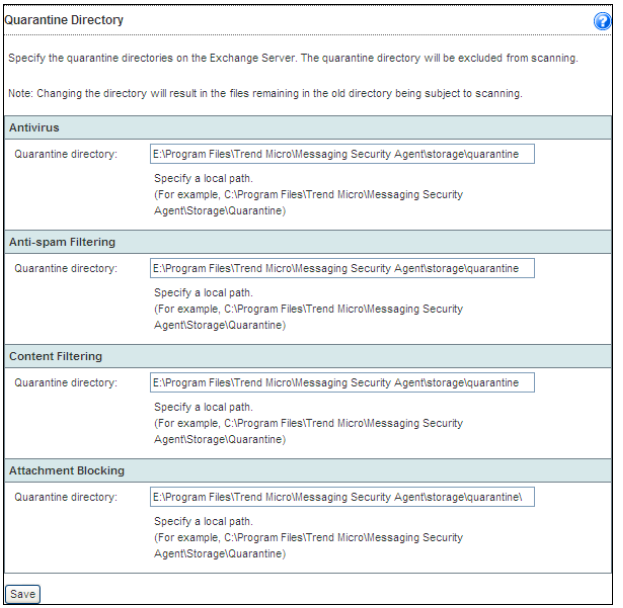


FIGURE 6-6. Quarantine Directory screen

To set up the Quarantine Directory

1. From the **Quarantine Directory** screen, set the directory path for the following quarantine folders:
   - **Antivirus**
   - **Anti-Spam**
   - **Content Filtering**
   - **Attachment Blocking**

   Refer to *Quarantine Directories* on page 6-41 for more information.
2. Click **Save**.

Querying Quarantine Directories

To view information about quarantined messages, query the Quarantine Directories.

Navigation Path: Security Settings > Select a Microsoft Exchange Server > **Configure > Quarantine > Query**

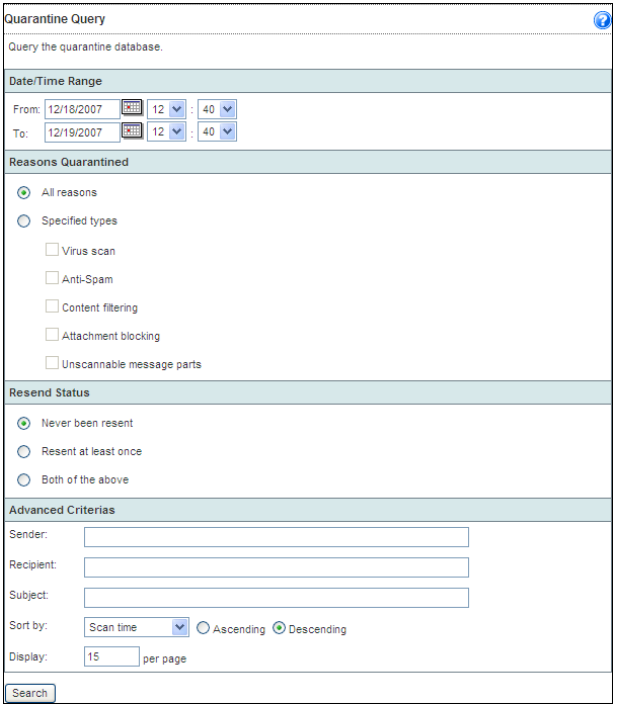


FIGURE 6-7. Quarantine Query screen

To query the Quarantine Directories:

1. 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.** Refer to *Quarantined Messages* on page 6-44 for more information.

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. To run a query, refer to *Querying Quarantine Directories* on page 6-43.

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.*

FIGURE 6-8. 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` (*Restore Encrypted Virus* on page 14-8) 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.

To delete a quarantined message:

Select the message and click  .

Tip: Configure Worry-Free Business Security Advanced to periodically delete quarantined messages. Refer to *Maintaining Quarantine Directories* on page 6-46 for more information.

Maintaining Quarantine Directories

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.

Navigation Path: Security Settings > Select a Microsoft Exchange Server > **Configure > Quarantine > Maintenance**

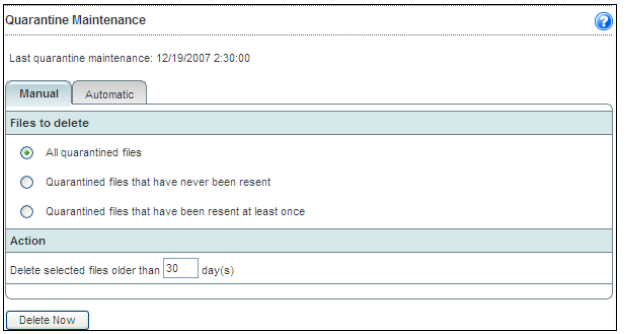


FIGURE 6-9. Quarantine Maintenance screen

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 Messaging Security Agent 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 Messaging Security Agent 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 Messaging Security Agent. End users can view this spam folder to open, read, or delete the suspect email messages. See *Setting up the Spam Folder* on page 6-48.

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 they click **Approved Sender**, the Messaging Security Agent moves the message from that sender to their inbox, adds the address of the message to their personal Approved Sender List. Clicking **View Approved Sender List** opens another screen that allows the end user to view and modify their list of approved senders by 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.

Note: Worry-Free Business Security Advanced also provides Administrators with an Approved Senders and Blocked Senders list. The Messaging Security Agent applies

the Administrator's approved senders and blocked senders before considering the end user list.

End User Quarantine Housekeeping Feature

The Messaging Security Agent 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 Messaging Security Agent and requires no configuration.

Setting up the Spam Folder

Open the Spam Maintenance screen by clicking **Operations > Spam Maintenance**.

Because the Messaging Security Agent identifies the folder by ID, not by folder name, end users can rename the spam folder (through Microsoft Outlook) without consequence.

You can set the following features from this screen:

- Disable the End User Quarantine tool
  Clear **Enable End User Quarantine tool** to disable the End User Quarantine tool for all mailboxes.
- Disable the End User Quarantine tool for one or more individual users
  This disables the End User Quarantine tool for each user you add to the **End User Quarantine tool exception list**.
- Create a new Spam Folder
  Create a new spam folder for each new user that you add to the Microsoft Exchange server where you installed the End User Quarantine tool.
- Modify the amount of days that the Messaging Security Agent will retain spam messages

See *Operations* on page 6-49 for more information about the End User Quarantine tool.

To create the spam folder:

1. Click **Operations > Spam Maintenance**.
2. Select **Enable End User Quarantine tool**.
3. Click **Create spam folder and delete spam messages.**
4. Click **Save.**

To reset the storage time limit:

1. Click **Operations > Spam Maintenance**.
2. Type the number of days you want the Messaging Security Agent 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).
3. Click **Save**.

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

1. Click **Operations > Spam Maintenance**.
2. Under **End User Quarantine tool exception list**, type the email address of the end-user for whom you want to disable EUQ.
3. Click **Add**. The end user's email address is added to the list of addresses that have EUQ disabled.
4. 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**.
5. Click **Save**.

Operations

During installation, Messaging Security Agent 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 Messaging Security Agent. 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**, Messaging Security Agent 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

Worry-Free Business Security Advanced 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.

Navigation Path: Security Settings > Select a Microsoft Exchange Server > **Configure > Operations > Notification Settings**

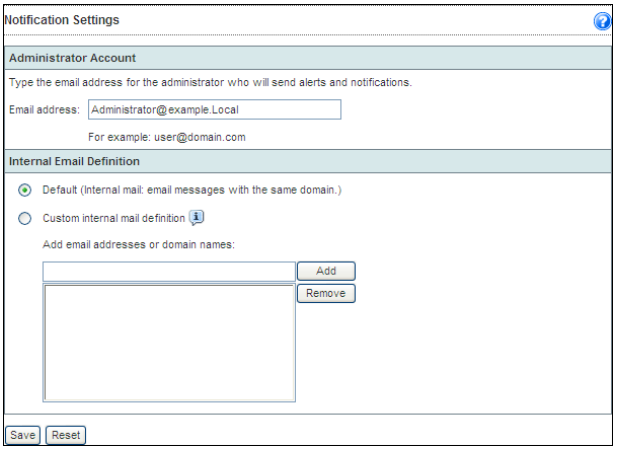


FIGURE 6-10. Notification Settings screen

To configure notification settings:

1. From the **Notification Settings** screen, update the following as required:
   - Email address. The address on behalf of whom Worry-Free Business Security Advanced will send notification messages.
   - **Internal Email Definition**
     - **Default:** Worry-Free Business Security Advanced 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

The **Spam Maintenance** screen displays the name of the Spam Folder and the number of days that the End User Quarantine (EUQ) tool retains spam messages. End users can rename the spam folder using Microsoft Outlook. Worry-Free Business Security identifies the folder by ID, not by folder name.

Note: EUQ and the **Spam Maintenance** screen are available only for Microsoft Exchange 2000 and 2003. In addition, if users choose Junk E-mail over EUQ during installation, the **Spam Maintenance** screen will be not display on the Web console. Without EUQ, Junk E-mail manages detected spam.

Navigation Path: Security Settings > Select a Microsoft Exchange Server **> Configure > Operations > Spam Maintenance**

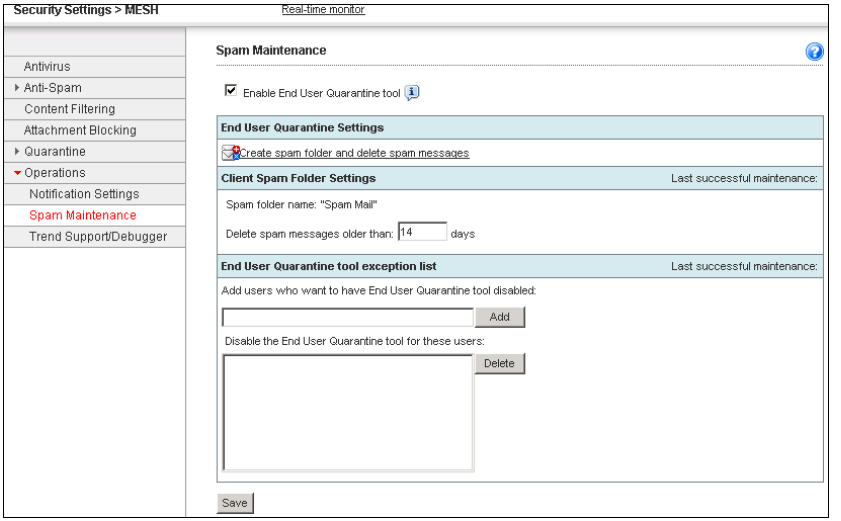


FIGURE 6-11. Spam Maintenance screen

To maintain spam:

1. 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. Refer to *POP3 Mail Scan* on page 5-23.

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 Debugger can assist you in debugging or just reporting the status of the Messaging Security Agent 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 Messaging Security Agent 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

Generate debugger reports to assist Trend Support in troubleshooting your problem.

To generate reports using the Debugger:

Navigation Path: Security Settings > Select a Microsoft Exchange Server > **Configure > Operations > Trend Support/Debugger**

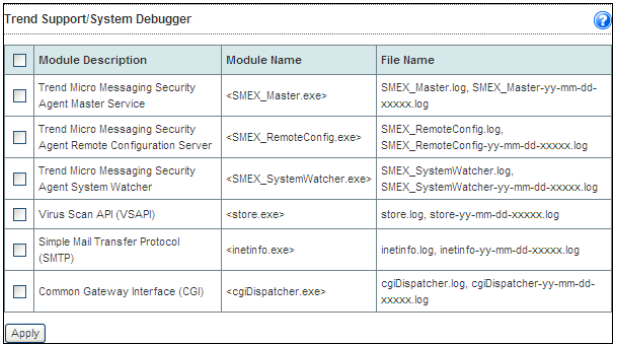


FIGURE 6-12. Trend Support/System Debugger screen

1. 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)**

   Refer to *Trend Support/Debugger* on page 6-53 for information about each module.
2. 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**.

Chapter 7

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 7-2
- *Current Status* on page 7-3
- *Potential Threat* on page 7-9
- *Setting up Outbreak Defense* on page 7-11

Outbreak Defense Strategy

Outbreak Defense is a key component of Worry-Free Business Security Advanced solution and protects your business during a worldwide threat outbreak.

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

TABLE 7-1. Outbreak Defense Response to the Outbreak Life Cycle Stages

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

Outbreak Defense Actions

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

- Blocking shared folders to help prevent virus/malware from infecting files in shared folders

- Blocking file with certain extensions on the Microsoft Exchange Server
- Adding content filtering rules to the Messaging Security Agent
- 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 virus cleanup engine
- Performing a **Cleanup** on all the Clients affected by the outbreak
- If enabled, scanning your Clients and networks and takes action against detected threats

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:

- Threat Prevention
- Threat Protection

- Threat Cleanup

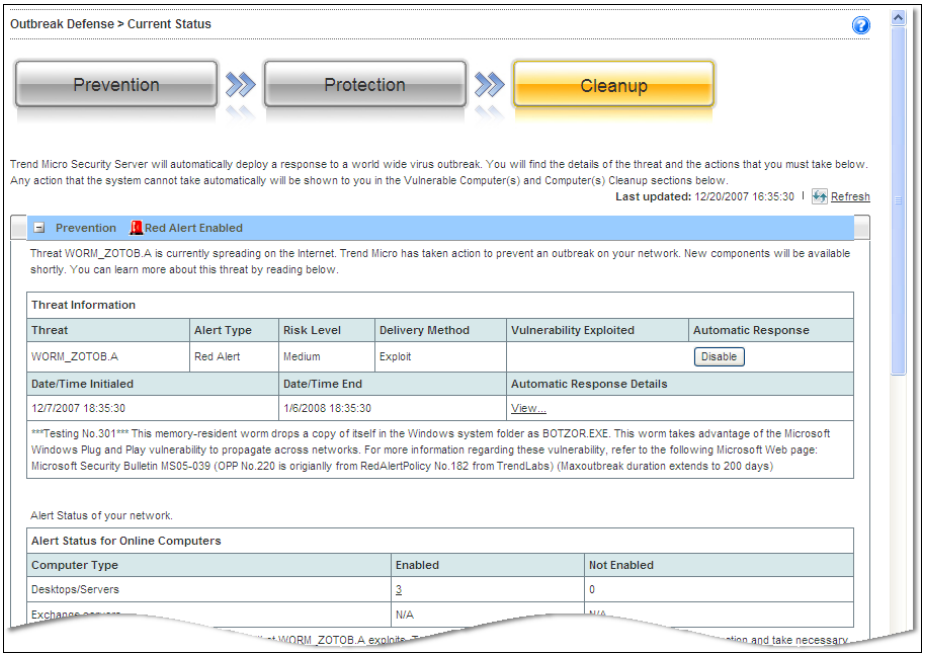


FIGURE 7-1. Outbreak Defense screen—No Threat

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.

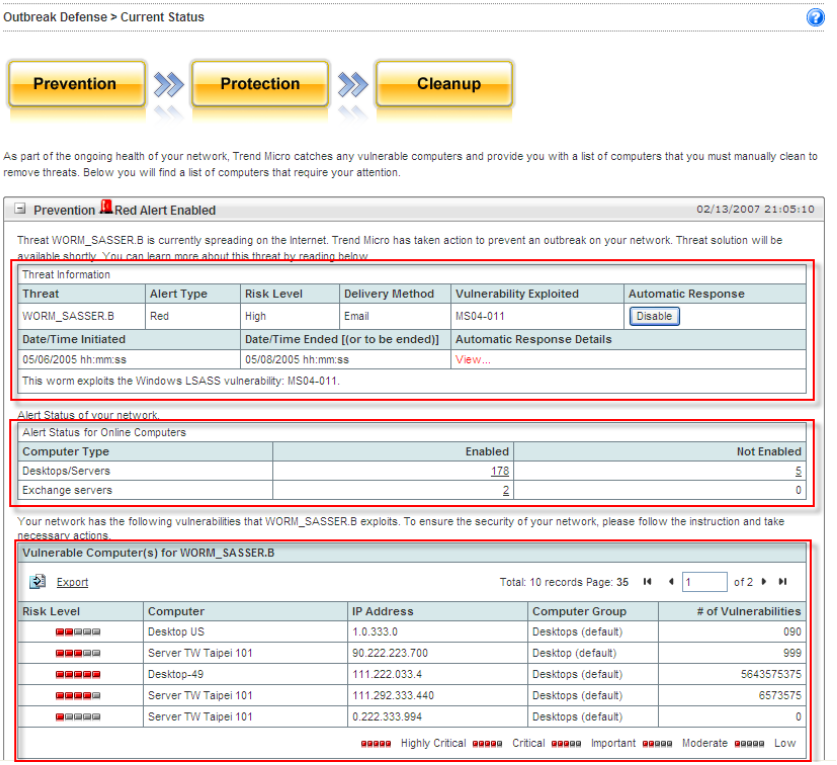


FIGURE 7-2. Outbreak Defense screen—Threat Prevention Stage

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 *Trend Micro*

Outbreak Prevention Policy on page C-2). Learn more about a threat by clicking **Help > Security Info** to redirect your browser to the Trend Micro Web site.

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.

Note: After you disable Outbreak Defense, Trend Micro recommends running Cleanup Now to help rid Clients of Trojans and any running processes related to Trojans or other types of malicious code (see *Computers to Cleanup* on page 7-10).

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.

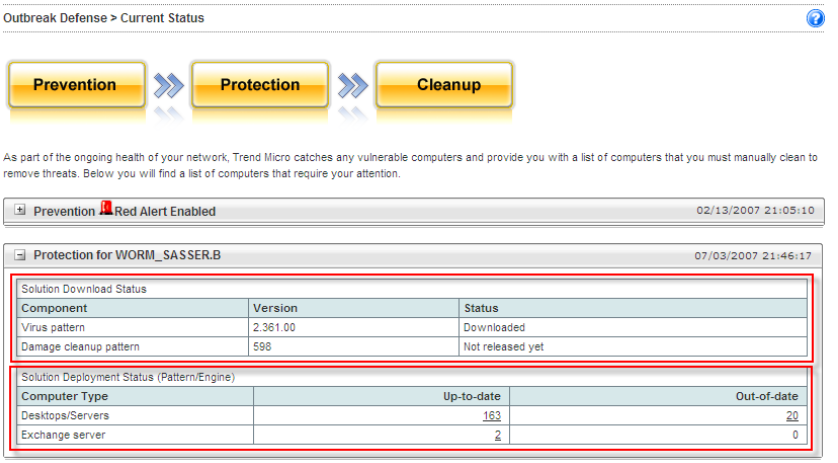


FIGURE 7-3. Outbreak Defense screen—Protection Stage

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.

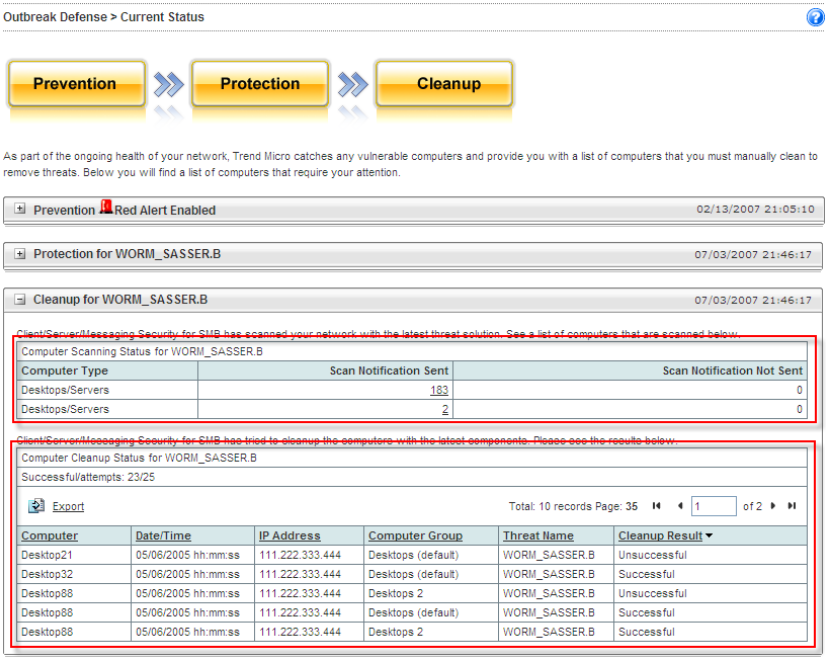


FIGURE 7-4. Outbreak Defense screen - Cleanup Stage

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.

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.

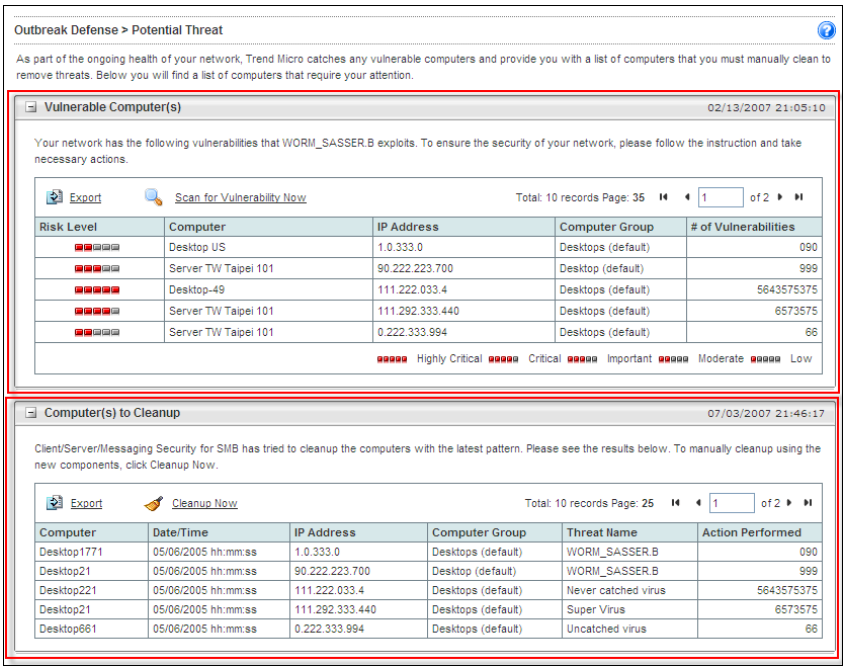


FIGURE 7-5. Potential Threat screen

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**, Worry-Free Business Security Advanced 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.

For additional information, refer to *Trend Micro Vulnerability Assessment* on page C-3.

Computers to Cleanup

Cleanup runs in the background whenever Agents run Antivirus scans. You do not need to set up scheduled Cleanup scans.

Client/Server Security Agents use Cleanup to protect Clients against Trojan horse programs (or Trojans). To address the threats and nuisances posed by Trojans and other virus/malware, Cleanup does the following:

- Detects and removes live Trojans and other virus/malware applications
- Kills processes that Trojans and other virus/malware applications create
- Repairs system files that Trojans and other virus/malware modify
- Deletes files and applications that Trojans and other virus/malware create

To accomplish these tasks, Cleanup makes use of:

- **Virus Cleanup Engine:** The engine Cleanup uses to scan for and remove Trojans and Trojan processes, worms, and spyware/grayware.
- **Virus Cleanup Pattern:** Used by the Virus Cleanup Engine. This template helps identify Trojans and Trojan processes, worms, and spyware/grayware, so the virus cleanup engine can eliminate them.

Cleanup runs on Clients when:

- Users perform a manual cleanup from the Agent
- Administrators perform Cleanup Now on Clients from the Web console
- 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 operates because it runs in the background (when Agents are running). However, the Security Server may sometimes notify the user to restart their Client to complete the cleanup. To learn more about how Damage Cleanup works, see *Trend Micro Damage Cleanup Services* on page C-2.

Setting up Outbreak Defense

Use the **Settings** screen to configure Outbreak Defense and Vulnerability Assessment options.

Outbreak Defense Settings

Worry-Free Business Security Advanced 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.

Red Alerts

Several business units have reported about a rapidly spreading virus/malware. As a response, Trend Micro has triggered 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 are received from several business units as well as support calls confirming scattered instances. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download. In case of an email-spreading virus/malware, content filtering rules, called Outbreak Prevention Policies (OPP), are sent out to automatically block related attachments on servers equipped with the product functionality.

Recommended Outbreak Defense Settings

The following settings are provided for optimal protection:

TABLE 7-2. 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	Enabled
Enable Automatic Outbreak Defense for Yellow Alerts issued by Trend Micro	Disabled
Disable Yellow Alerts after	NA
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	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

Configuring Outbreak Defense Settings

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.

Navigation Path: Outbreak Defense > Settings > Outbreak Defense tab

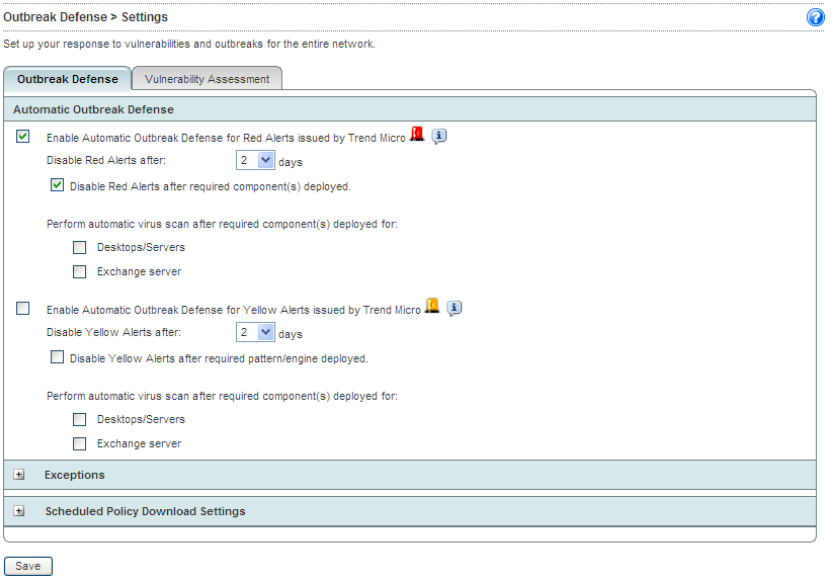


FIGURE 7-6. Outbreak Defense tab of Outbreak Defense Settings screen

To configure the Outbreak Defense settings:

1. 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
  - Microsoft Exchange Servers
- **Yellow Alert settings:** Configure the options for Yellow Alerts. Refer to *Yellow Alerts* on page 7-12 for more information.
- **Exceptions:** The ports that will not be blocked during Outbreak Defense Automatic Response. Refer to *Using Outbreak Defense Exceptions* on page 7-15 to work with Exceptions.

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.**

Using Outbreak Defense Exceptions

Use Exceptions to Add, Edit or Remove ports from being excluded from blocking.

Navigation Path: Outbreak Defense > Settings > Outbreak Defense tab

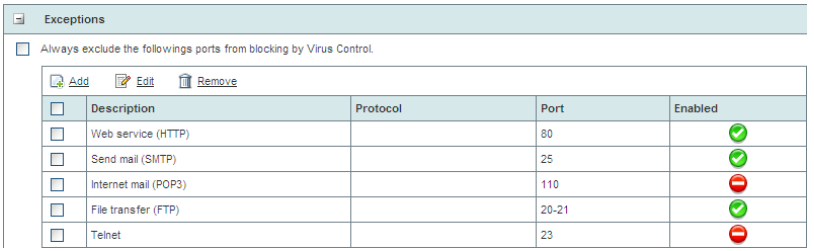


FIGURE 7-7. Exceptions section of Outbreak Defense Settings screen

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:** A brief description that will help identify the exception.
   - **Protocol:** Select the protocol to which the exception must be applied.
   - **Ports:** Type a port range or individual ports for the exception. Separate multiple entries with semicolons (;).
4. Click **Add.**

To edit an exception:

1. Click the plus **(+)** icon for the **Exceptions** section.
2. Select the exception and click **Edit.**
3. Update the options as required.
4. Click **Save.**

To remove an exception:

Tip: Disable an Exception instead of removing.

---

1. Click the plus **(+)** icon for the **Exceptions** section.
2. Select the exception and click **Remove.**
3. Click **OK** to confirm.

Configuring Vulnerability Assessment Settings

The Vulnerability Assessment settings determine the frequency and the target of the Vulnerability Prevention scans.

Navigation Path: Outbreak Defense > Settings > Vulnerability Assessment tab

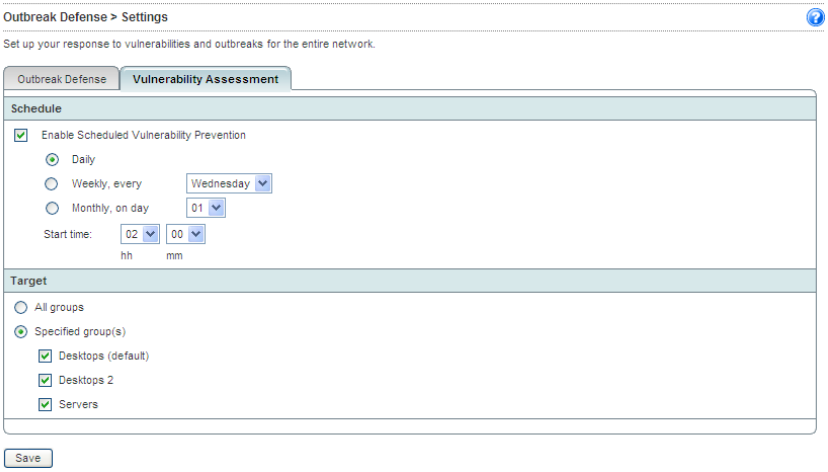


FIGURE 7-8. Vulnerability Assessment tab of Outbreak Defense Settings screen

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 Security Settings screen.
     - **Specified group(s):** Limit the vulnerability assessment scan to only the selected groups.
2. Click **Save**.

Chapter 8

Configuring Manual and Scheduled Scans

This chapter describes how to use Manual and Scheduled scans to protect your network and Clients from virus/malware and other threats.

The topics discussed in this chapter include:

- *Worry-Free Business Security Advanced Scans* on page 8-2
- *Scanning Clients* on page 8-3

Worry-Free Business Security Advanced Scans

Worry-Free Business Security Advanced provides three types of scans to protect your Clients from Internet threats: Manual Scan, Scheduled Scan, and Real-time Scan. Each scan has a different purpose and use, but all are configured approximately the same way. This chapter discusses Manual and Scheduled Scans.

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 removes 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 amount of time it takes to scan depends on the Client's hardware resources and the number of files to be scanned.

Configure the Antivirus, Content Filtering, and Attachment Blocking options for Manual Scans. To configure a Manual Scan, click **Scans > Manual Scan**. Refer to *Configuring Scan Options for Groups* on page 8-3 and *Configuring Scan Options for Microsoft Exchange Servers* on page 8-8 for more information.

Scheduled Scan

A Scheduled Scan is similar to Manual Scan except that it scans all files and email messages at the configured time and frequency. Use Scheduled Scans to automate routine scans on your Clients and improve the efficiency of threat management.

To configure a Scheduled scan, click **Scans > Scheduled Scan**. Refer to *Scheduling Scans* on page 8-12 for more information.

Real-time Scan

Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for threats. Refer to *Configuring Real-time Scan* on page 5-5 for more information. In the case of email

messages, the Messaging Security Agent guards all known virus entry points with Real-time Scanning of all incoming messages, SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers. Refer to *Antivirus* on page 6-7.

Scanning Clients

The following section explains how to configure both Manual and Schedule Scans for Clients. For instructions to schedule a Scheduled Scan, refer to *Scheduling Scans* on page 8-12.

Navigation Path: Scans > Manual Scan or Scheduled Scan

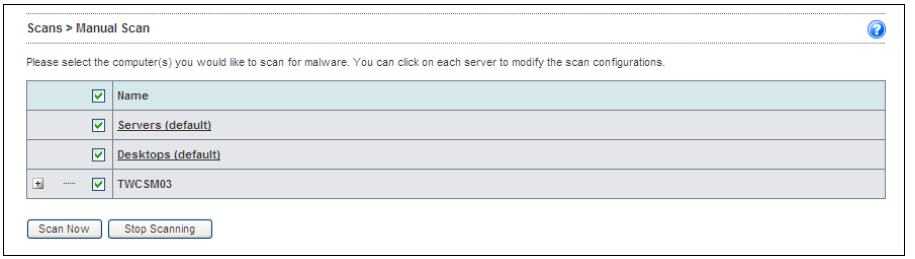


FIGURE 8-1. Manual Scan screen

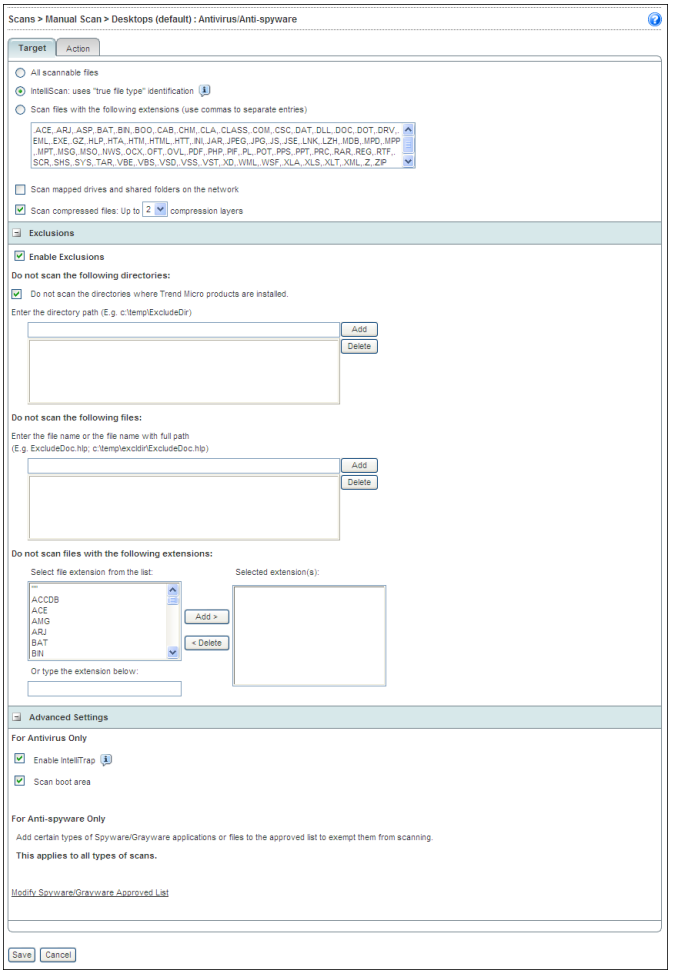
To configure Manual or Scheduled Scans for Clients:

1. From the **Manual Scan** or **Scheduled Scan** screen, select the groups to scan.
2. Set the scanning options for a group by clicking on the group name. Refer to *Configuring Scan Options for Groups* on page 8-3.
3. For Scheduled Scans, update the schedule on the **Schedule** tab. Refer to *Scheduling Scans* on page 8-12.
4. Click **Scan Now** or **Save**.

Configuring Scan Options for Groups

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

Navigation Path: Scans > Manual Scan or Scheduled Scan > Click a group



To configure the scan options:

1. From the group's scanning options screen, update the following as required:
   - Files to scan

- **All scannable files:** Only encrypted or password-protected files are excluded.
- **IntelliScan:** Scans files based on true-file type. Refer to *Trend Micro IntelliScan* on page C-4 for more information.
- **Scan files with the following extensions:** Worry-Free Business Security Advanced will scan files with the selected extensions. Separate multiple entries with commas (,).
- **Scan mapped drives and shared folders on the network**
- **Scan compressed files:** Configure the number of layers to scan.

- **Exclusions:** Exclude specific files, folders, or files with certain extensions from being scanned.
  - **Enable Exclusions**
  - **Do not scan the directories where Trend Micro products are installed**
  - **Folder exclusions:** Type the name of the folder to exclude from the scan. Click **Add.** To remove a folder, select the folder and click **Delete**.
  - **File exclusions:** Type the name of the file to exclude from the scan. Click **Add.** To remove a file, select the file and click **Delete**.
  - **Extension exclusions:** Type the name of the extension to exclude from the scan. Click **Add.** To remove an extension, select the extension and click **Delete**.
- **Advanced Settings**
  - **Enable IntelliTrap** (for antivirus)**:** IntelliTrap detects malicious code such as bots in compressed files. Refer to *Trend Micro IntelliTrap* on page C-6 for more information.
  - **Scan boot area** (for antivirus)**:** The boot sector contains the data used by Clients to load and initialize the operating system. A boot sector virus infects the boot sector of a partition or a disk.
  - **Spyware/Grayware Approved List** (for anti-spyware)**:** This list contains details of the approved spyware/grayware applications. Click the link to update the list. Refer to *Editing the Spyware/Grayware Approved List* on page 8-6 for more information.

2. From the **Action** tab, specify how Worry-Free Business Security Advanced should handle detected threats:

- **CPU Usage:** The period of time Security Server waits between scanning each file affects CPU usage. Select a lower CPU usage level to increase the wait time between file scans, which frees up the CPU to perform other tasks.
- Action for Virus Detections
  - **ActiveAction:** Use Trend Micro preconfigured actions for threats. Refer to *Trend Micro ActiveAction* on page C-4 for more information.
  - **Same action for all threats:** Select from Pass, Delete, Rename, Quarantine, or Clean. If you select Clean, set the action for an uncleanable threat.
  - **Customized action for the following detected threats:** Select from Pass, Delete, Rename, Quarantine, or Clean for each type of threat. If you select Clean, set the action for an uncleanable threat.
  - **Backup detected file before cleaning:** 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\Client Server Security Agent\Backup`

    To decrypt the file, refer to *Restore Encrypted Virus* on page 14-8
- Action for Spyware/Grayware Detections
  - **Clean:** When cleaning spyware/grayware, Worry-Free Business Security Advanced could delete related registry entries, files, cookies, and shortcuts. Processes related to the spyware/grayware could also be terminated.
  - **Pass:** Only logs the infection for further assessment. Refer to *Logs* **on page 10-2** for more information.

3. Click **Save**.

   Additionally, configure who receives notifications when an event occurs. Refer to *About Notifications* on page 11-2.

Editing 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. Refer to *Spyware/Grayware Types* on page E-1 to learn about the different kinds of spyware.

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

Navigation Path: Scans > Manual Scan or Scheduled Scan > Click a group **> Advanced Settings**

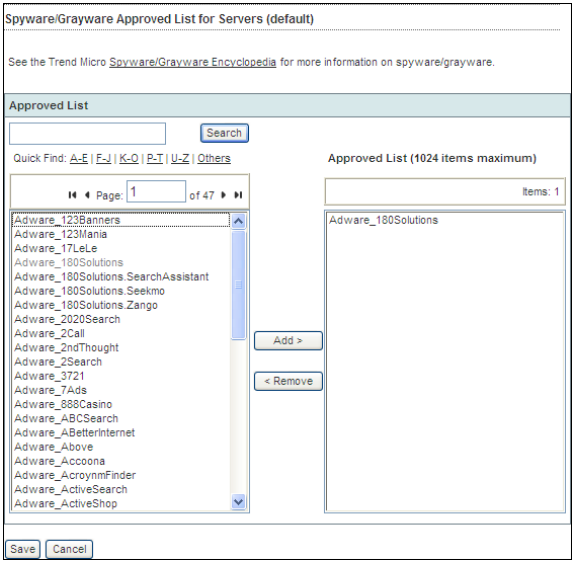


FIGURE 8-2. Spyware/Grayware Approved List screen

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.
- **<Remove**

3. Click **Save**.

Configuring Scan Options for Microsoft Exchange Servers

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

Navigation Path: Scans > Manual Scan or Scheduled Scan > Expand a Microsoft Exchange Server **> Antivirus/Content Filtering/Attachment Blocking**

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:** Refer to *Configuring Antivirus Scan Options for Microsoft Exchange Servers* on page 8-9 for more information.
   - **Content Filtering:** Refer to *Configuring Content Filtering Options for Microsoft Exchange Servers* on page 8-12 for more information.
   - **Attachment Blocking:** Refer to *Configuring Attachment Blocking Options for Microsoft Exchange Servers* on page 8-12 for more information.
3. For Scheduled Scans, update the schedule on the **Schedule** tab. Refer to *Scheduling Scans* on page 8-12.
4. Click **Scan Now** or **Save**.

Configuring Antivirus Scan Options for Microsoft Exchange Servers

Configuring antivirus scan options for Microsoft Exchange servers involves setting the Target (threats to scan) and the Action (action for detected threats).

Navigation Path: Scans > Manual Scan or Scheduled Scan > Expand a Microsoft Exchange Server **> Antivirus**

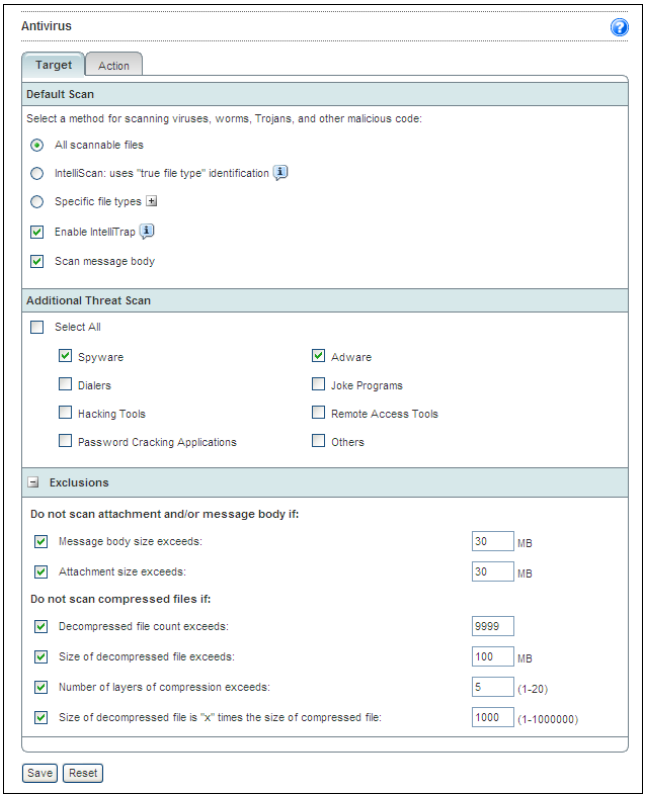


FIGURE 8-3. Antivirus Scan Options for Microsoft Exchange Server

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 following 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. Refer to *Glossary of Terms* **on page F-1** for definitions of threats.
- **Exclusions:** Exclude email messages that match the following criteria from scans:
  - Message body size exceeds specified size
  - Attachment size exceeds specified size
  - Decompressed file count exceeds specified size
  - Size of decompressed file exceeds specified size
  - Number of layers of compression exceeds specified size
  - 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. Refer to *Trend Micro ActiveAction* on page C-4 for more information.
     - **Same action for all threats:** Select from Clean, Replace with Text/File, Delete Entire message, Pass, or Quarantine 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 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, refer to *Restore Encrypted Virus* on page 14-8
- **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. Refer to *Advanced Macro Scanning* on page 6-5 for more information.
- **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 (refer to the section on setting exclusions on page 8-10). 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.**

   Additionally, configure who receives notifications when an event occurs. Refer to *About Notifications* on page 11-2.

Configuring Content Filtering Options for Microsoft Exchange Servers

Configuring content filtering options for Microsoft Exchange servers involves setting the rules to block messages with certain content.

Navigation Path: Scans > Manual Scan or Scheduled Scan > Expand a Microsoft Exchange Server **> Content Filtering**

Refer to *Content Filtering* on page 6-20 for more information.

Configuring Attachment Blocking Options for Microsoft Exchange Servers

Configuring attachment blocking options for Microsoft Exchange servers involves setting the rules to block messages with certain attachments.

Navigation Path: Scans > Manual Scan or Scheduled Scan > Expand a Microsoft Exchange Server **> Attachment Blocking**

Refer to *Attachment Blocking* on page 6-35 for more information.

Scheduling Scans

Schedule scans to periodically scan Clients and Microsoft Exchange servers for threats.

Tip: Trend Micro recommends that you not schedule 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**.

Navigation Path: Scans > Scheduled Scan > Schedule tab

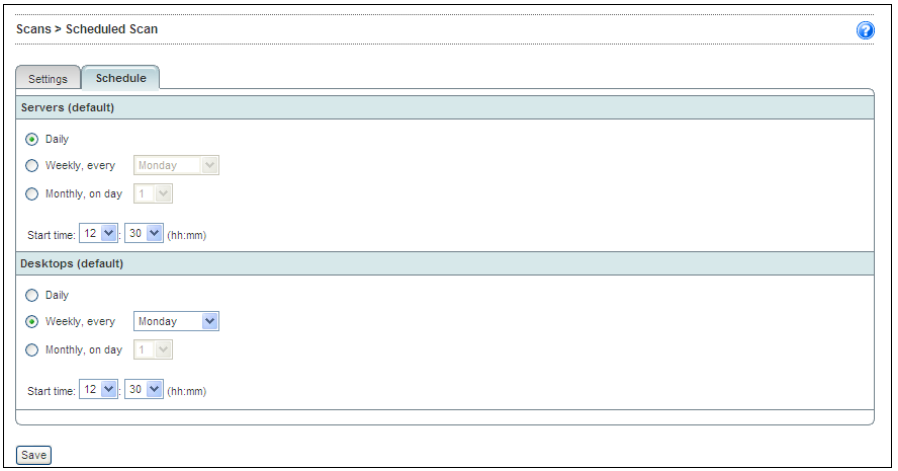


FIGURE 8-4. Scheduled Scan screen

To schedule a scan:

1. Before scheduling a scan, configure the settings for the scan. Refer to *Configuring Scan Options for Groups* on page 8-3 and *Configuring Scan Options for Microsoft Exchange Servers* on page 8-8 for more information.
2. From the **Scheduled** tab, update the following options for each group or Microsoft Exchange server 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, Worry-Free Business Security Advanced 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. Refer to *About Notifications* on page 11-2.

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

Chapter 9

Updating Components

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

- *Updating Components* on page 9-2
- *Updatable Components* on page 9-3
- *Update Sources* on page 9-6
- *Manual and Scheduled Updates* on page 9-11
- *Rolling Back or Synchronizing Components* on page 9-14

Updating Components

Worry-Free Business Security Advanced makes upgrading to the latest components easy by having Agents automatically receive updated components from the Security Server.

Worry-Free Business Security Advanced downloads components from the Trend Micro ActiveUpdate Server (see *About ActiveUpdate* on page 9-3 for more information):

- When you install the product for the first time, all of components for the Security Server and Agents are immediately updated from the Trend Micro ActiveUpdate Server.
- Whenever the Worry-Free Business Security Advanced master service is started, ActiveUpdate server is checked to see if updates are available.
- By default, Scheduled Updates run every hour to update the Security Server.
- By default, Messaging Security Agent runs a Scheduled update once every 24 hours at 12:00 AM.
- By default, Client/Server Security Agent runs a Scheduled update every eight hours.

Tip: To ensure that Client/Server Security Agents stay up-to-date even when not connected to the Security Server, set Client/Server Security Agents to receive updates from an alternative source (*Configuring an Update Source* on page 9-8). This is useful for end users who are often away from the office and disconnected from the local network.

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

About ActiveUpdate

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

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 Worry-Free Business Security Advanced

Click Trend Micro's ActiveUpdate Server from the **Updates > Update 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.

Updatable Components

To ensure Clients stay protected from the latest threats, update the Worry-Free Business Security Advanced components regularly.

Configure the Security Server to download Worry-Free Business Security Advanced components from the ActiveUpdate server. The ActiveUpdate server provides updated components such as the virus pattern files, scan engines, and program files. After the server downloads any available updates, it automatically deploys the updated components to the Agents.

Worry-Free Business Security Advanced provides two methods for updating your components:

- Update your components manually, see *Manually Updating Components* on page 9-12.

- Update your components based on a schedule, see *Scheduling Component Updates* on page 9-13.

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 12-2.

TABLE 9-1. Updatable Components

Component	Sub-component
Antivirus	• Virus Pattern • Virus Scan Engine 32-bit • Virus Scan Engine 64-bit • Virus Cleanup Template • Virus Cleanup Engine 32-bit • Virus Cleanup Engine 64-bit • Messaging Security Agent Scan Engine 32-bit • Messaging Security Agent Scan Engine 64-bit • IntelliTrap Exception Pattern • IntelliTrap Pattern
Anti-spyware	• Spyware Scan Engine 32-bit • Spyware Scan Engine 64-bit • Spyware Pattern • Spyware Active-monitoring Pattern
Anti-spam	• Anti-spam Pattern • Anti-spam Engine 32 -bit • Anti-spam Engine 64-bit
Outbreak Defense	• Vulnerability Pattern
Network Virus	• Common Firewall Pattern • Common Firewall Engine 32-bit • Common Firewall Engine 64-bit • TDI Driver 32-bit • TDI Driver 64-bit • WFP Driver 32-bit • WFP Driver 64-bit
Web Threat Protection	• URL Filtering Engine 32-bit • URL Filtering Engine 64-bit

TABLE 9-1. Updatable Components

Component	Sub-component
Behavior Monitoring	• Behavior Monitor Core Drivers 32-bit • Behavior Monitor Core Service 32-bit • Policy Enforcement Pattern • White Listing Pattern • Behavior Monitor Configuration Pattern

Refer to *About Components* on page 1-17 for detailed information about each component.

Default Update Times

By default, Worry-Free Business Security Advanced checks for updates and downloads components, if necessary, from the Trend Micro ActiveUpdate Server under the following circumstances:

- When you install the product for the first time, all the components for the Security Server and Agents are immediately updated from the Trend Micro ActiveUpdate Server.
- Whenever the Worry-Free Business Security Advanced master service is started, the Security Server updates the Outbreak Defense policy.
- By default, Scheduled Updates run every hour to update the Security Server.
- To ensure that Agents stay updated, Client/Server Security Agent runs a scheduled update every 8 hours.

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

Generally, Trend Micro updates the scan engine or program only during the release of a new Worry-Free Business Security Advanced version. However, Trend Micro releases pattern files frequently.

Updating the Security Server

Worry-Free Business Security Advanced automatically performs the following updates:

- When you install the product for the first time, all components for the Security Server and Clients are immediately updated from the Trend Micro ActiveUpdate server.
- Whenever the Worry-Free Business Security Advanced starts, the Security Server updates the components and the Outbreak Defense policy.
- By default, Scheduled Updates run every hour.
- To ensure that Clients stay up-to-date, Agents run a scheduled update every 8 hours.

To configure Trend Micro Security Server to perform updates:

1. Select an update source. Refer to *Update Sources* on page 9-6.
2. Configure the Trend Micro Security Server for manual or scheduled updates. Refer to *Manual and Scheduled Updates* on page 9-11.
3. Use **Client Privileges** to configure update options for Clients running the Client/Server Security Agent and/or the Messaging Security Agent. Refer to *Client Privileges* on page 5-25.

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 9-2. Update Source options

Update Option	Description	Recommendation
ActiveUpdate server > Trend Micro Security Server > 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".

TABLE 9-2. Update Source options

Update Option	Description	Recommendation
ActiveUpdate server > Trend Micro Security Server > Update Agents > 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”.
ActiveUpdate server > Update Agents > Clients	Update Agents receive updated components directly from the ActiveUpdate server (or another Update Agent) and deploy them to Clients.	Use this method only if you are experiencing problems updating Update Agents from the Trend Micro Security Server or from other Update Agents. Under most circumstances, Update Agents receive updates faster from the Trend Micro Security Server or from other Update Agents than from an external update source.

Configuring an Update Source

Navigation Path: Updates > Source

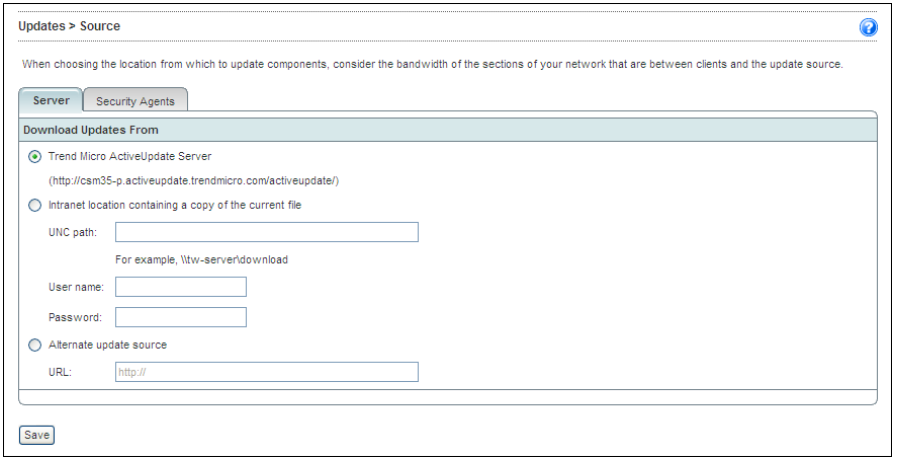


FIGURE 9-1. Update Source screen

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. Select the ActiveUpdate server as a source if you require frequent and timely updates.

   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**.

Using Update Agents

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.

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.

Navigation Path: Updates > Source > Security Agents tab

To allow Agents to act as Update Agents:

1. From the **Security Agents** tab on the **Source** screen, click **Add** in the **Assign Update Agents** section.
2. From the **Select Security Agents** list box, select one or more Agents to act as Update Agents.
3. 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 **Security 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 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 add alternative update sources:

1. From the **Security 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 Client/Server Security Agent, enter the Client/Server 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.
     - **Specified:** The path to an Update Agent or an ActiveUpdate server.
3. Click **Save**.

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

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

Manual and Scheduled Updates

Worry-Free Business Security Advanced offers two methods to update the different components.

Manual Updates

Trend Micro recommends updating the server manually immediately after deploying a Client/Server Security Agent and whenever there is a virus/malware outbreak.

Scheduled Updates

Configure the Trend Micro Security Server to regularly check its update source and automatically download any available updates. Because Agents normally get updates from the Trend Micro Security Server, using automatic scheduled update is an easy and effective way of ensuring that your protection against virus/malware is always current. Setting Scheduled updates is similar to setting Manual updates, both procedures will be combined here. An additional section for setting an update time will follow.

Tip: Trend Micro recommends frequently updating components.

Manually Updating Components

Navigation Path: Updates > Manual Update

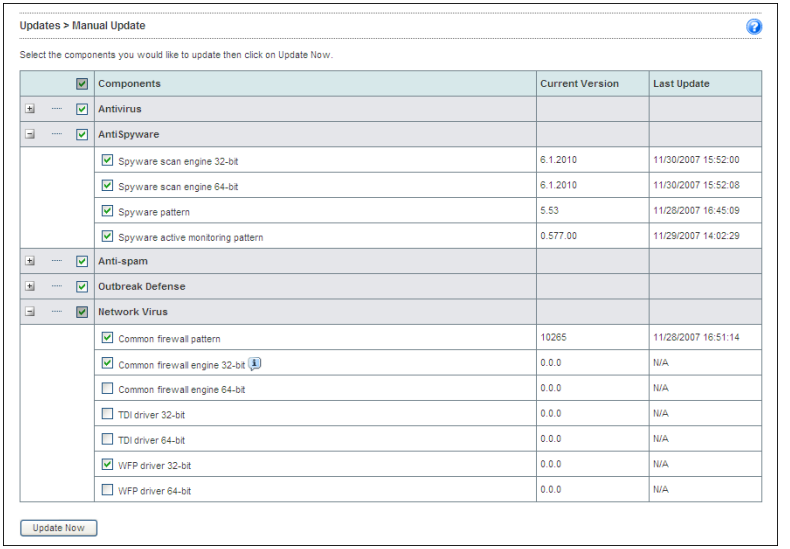


FIGURE 9-2. Manual Update screen

To manually update components:

1. 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 the components to update and select the corresponding check boxes. For information about each component, refer to *Updateable Components* on page 1-28.
2. Click **Update Now** or **Save.** If scheduling updates, refer to *Scheduling Component Updates* on page 9-13.

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

Scheduling Component Updates

Schedule updates to automatically receive the latest components to combat threats.

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

Navigation Path: Updates > Scheduled Scan > Schedule tab

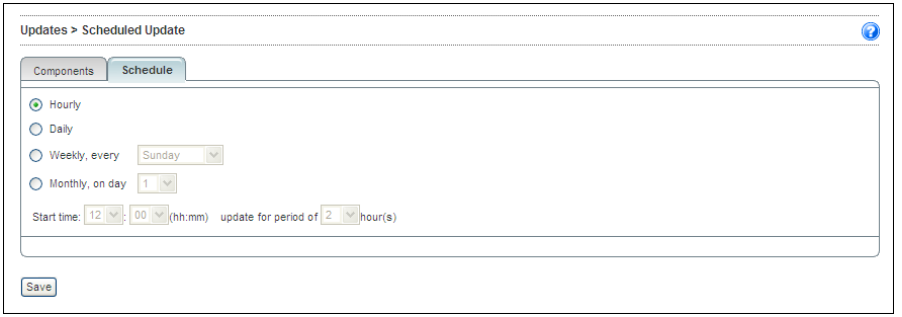


FIGURE 9-3. Scheduled Update screen

To schedule an update:

1. From the **Components** tab on the **Scheduled Update** screen, update the following as required:
   - **Components:** To select all components, select the Components check box. To select individual components, click ⊞ to display the components to update and select the corresponding check boxes. For information about each component, refer to *Updateable Components* on page 1-28.
2. From the **Scheduled Update** tab, update the following options as required:
   - **Hourly:** Checks for updates every hour.
   - **Daily:** The Scheduled Update runs every day at the **Start time**.
   - **Weekly, every:** The Scheduled Update runs once a week on the specified day at the **Start time**.
   - **Monthly, on day:** The Scheduled Update runs once a month on the specified day beginning at the **Start time**.

- **Start time:** The time the Scheduled Update should start.
- **Update period:** The period within which updates can run.

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.

Rolling Back or Synchronizing Components

Rolling back refers to reverting to the previous version of a virus pattern file or scan engine. If the pattern file or scan engine that you are using is not functioning properly, roll back these components to their previous versions.

Synchronizing refers to deploying the updated components to all Agents.

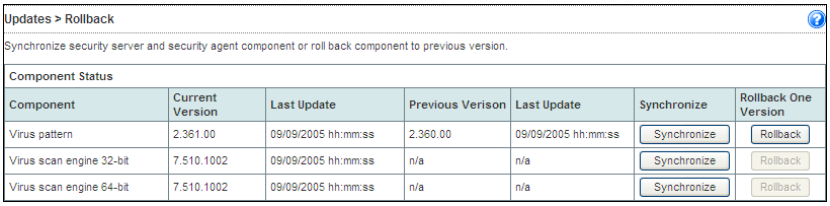
Note: You can roll back only the virus pattern file and scan engine. No other components can be rolled back.

The Agents use the following scan engines:

- Virus scan engine 32-bit
- Virus scan engine 64-bit

You need to roll back these types of scan engines separately. The rollback procedures for both types of scan engines are the same. The Trend Micro Security Server retains only the current and the previous versions of the scan engine and the last five pattern files.

Navigation Path: Updates > Rollback


Updates > Rollback

Synchronize security server and security agent component or roll back component to previous version.

Component Status

Component	Current Version	Last Update	Previous Verison	Last Update	Synchronize	Rollback One Version
Virus pattern	2.361.00	09/09/2005 hh:mm:ss	2.360.00	09/09/2005 hh:mm:ss	Synchronize	Rollback
Virus scan engine 32-bit	7.510.1002	09/09/2005 hh:mm:ss	n/a	n/a	Synchronize	Rollback
Virus scan engine 64-bit	7.510.1002	09/09/2005 hh:mm:ss	n/a	n/a	Synchronize	Rollback

FIGURE 9-4. Rollback screen

To roll back or synchronize pattern files or scan engines:

From the **Rollback** screen, select the following options as required:

- **Rollback:** reverts the Security Server and Agent components to the previous version.
- **Synchronize:** deploys the updated components to Agents.

Chapter 10

Viewing and Interpreting 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 10-2
- *Reports* on page 10-3
- *Managing Logs and Reports* on page 10-10
- *Generating Reports* on page 10-7
- *Managing Logs and Reports* on page 10-10

Logs

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

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

Worry-Free Business Security Advanced maintains logs under the following categories:

- Management console event logs
- Desktop/Server logs
- Microsoft Exchange server logs

TABLE 10-1. Log Type and Content

Type (event or item that generated the log entry)	**Content** (type of log to obtain content from)
Management console events	• Manual Scan • Update • Outbreak Defense events • Console events

Desktop/Server	• Virus logs
	  • Manual Scan
	  • Real-time Scan
	  • Scheduled scan
	  • Cleanup
	• Spyware logs
	  • Manual Scan
	  • Real-time Scan
	  • Scheduled scan
	• URL violation logs
	• Behavior monitoring logs
	• Update logs
	• Network virus logs
	• Outbreak Defense logs
	• Event logs

TABLE 10-1. Log Type and Content

Type (event or item that generated the log entry)	**Content** (type of log to obtain content from)
Microsoft Exchange server	• 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 log

Reports

This section explains how to configure both one-time and scheduled reports.

One-Time Reports

Generate One-time Reports to view log information in an organized and graphically appealing format.

Scheduled Reports

Contents of Scheduled Reports are similar to One-Time Reports, but are generated at the specified time and frequency. To generate scheduled reports, select the contents of the report and save it as a template. At the specified time and frequency, Worry-Free Business Security Advanced uses the template to generate the report.

Interpreting Reports

Worry-Free Business Security Advanced reports contain the following information. The information displayed could vary depending on the options selected.

TABLE 10-2. 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
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 Worry-Free Business Security Advanced 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 Web site.
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-spam summary	**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.

TABLE 10-2. Contents of a report

Report Item	Description
Content filtering summary	**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/malware. **Top 10 Computers Attacked** List the Clients on your network that report the most frequent virus/malware incidents.
Web Threat Protection	**Top 10 Computers Violating Web Threat Protection Policies** Lists the top 10 Clients that have violated Web Threat Protection policies.
Behavior Monitoring	**Top 5 Programs Violating Behavior Monitoring Policies** Lists the top five programs violating Behavior Monitoring policies. **Top 10 Computers Violating Behavior Monitoring Policies** Lists the top 10 Clients that have violated Behavior Monitoring policies.

Using Log Query

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

Note: An MSA sends its logs to the Security Server every five minutes (regardless of when the log is generated).

Navigation Path: Reports > Log Query

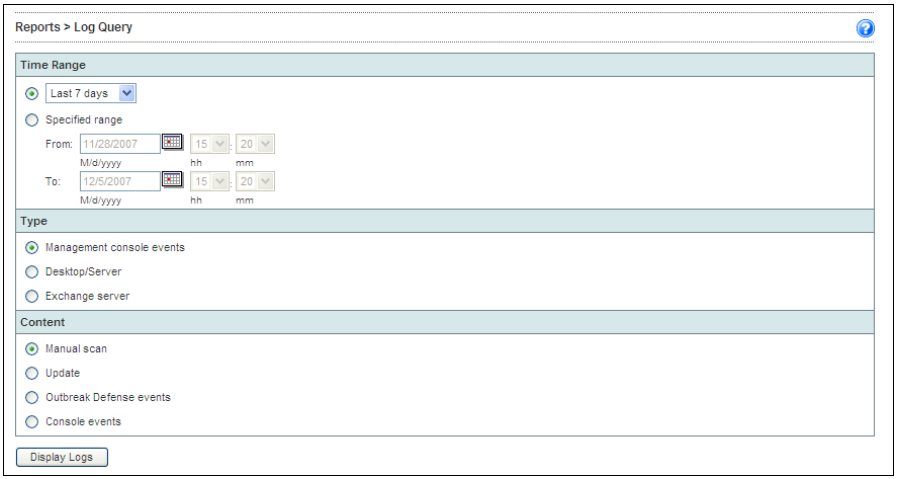


FIGURE 10-1. Default Log Query screen

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:** Refer to Table 10-1 on page 10-2 to view the contents of each log type.
     - **Management console events**
     - **Desktop/Server**
     - **Microsoft Exchange Server**
   - **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.

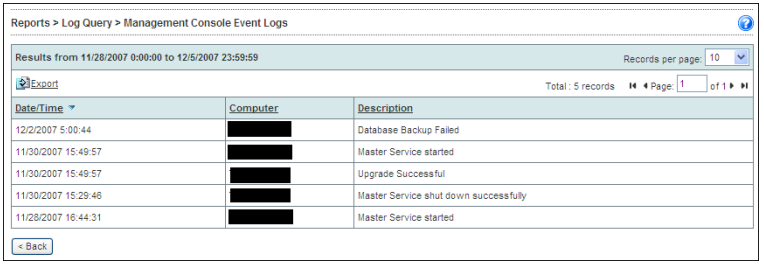
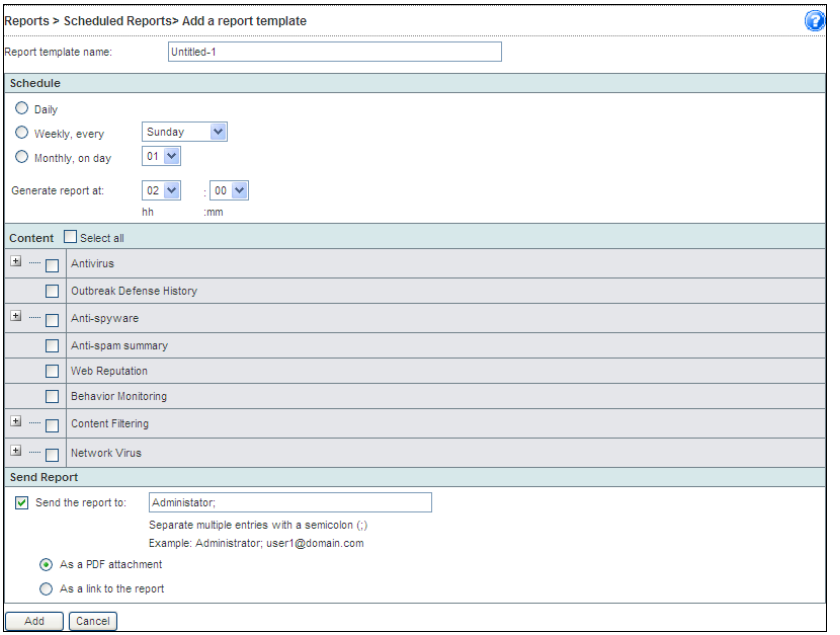


FIGURE 10-2. Sample Log Query screen

Generating Reports

One-time reports provide a summary of the selected content just once. Scheduled reports provide a summary of the selected content on a regular basis.

Navigation Path: Reports > One-time Reports or Scheduled Reports



To create or schedule a report:

1. From the **One-time Reports** screen or **Scheduled Report** screen, click **New Report**/**Add**.
2. Update the following options as required:
   - **Report Name/Report Template Name:** 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, Worry-Free Business Security Advanced will not generate the report that month.

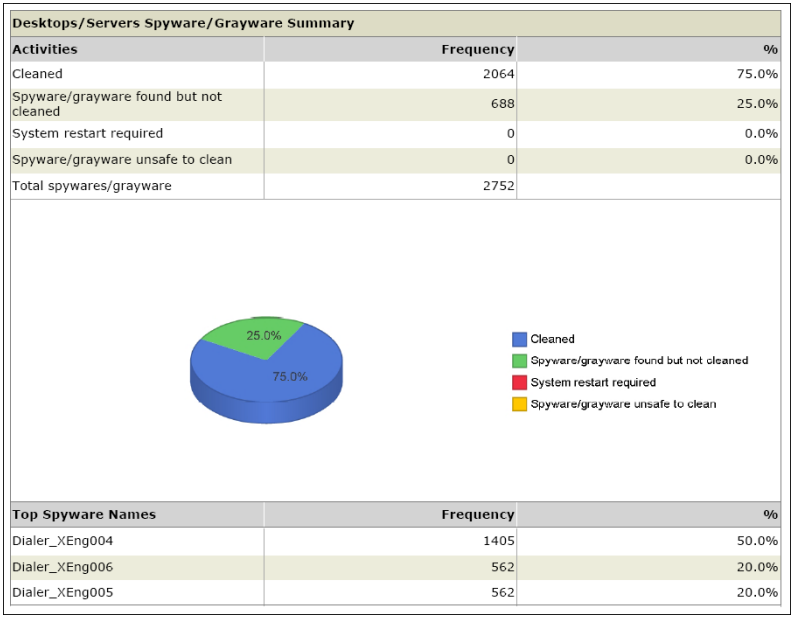
- **Generate report at:** The time Worry-Free Business Security Advanced should generate the report.

- **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:** Worry-Free Business Security Advanced 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**. View the report from the **One-Time Reports or Scheduled Reports** screen by clicking the name of the Report. If **Send the report to** is enabled, Worry-Free Business Security Advanced sends the PDF attachment or link to the recipients.

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

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



Desktops/Servers Spyware/Grayware Summary

Activities	Frequency	%
Cleaned	2064	75.0%
Spyware/grayware found but not cleaned	688	25.0%
System restart required	0	0.0%
Spyware/grayware unsafe to clean	0	0.0%
Total spywares/grayware	2752	

Top Spyware Names	Frequency	%
Dialer_XEng004	1405	50.0%
Dialer_XEng006	562	20.0%
Dialer_XEng005	562	20.0%

FIGURE 10-3. Sample report showing spyware/grayware summary

Managing Logs and Reports

Reports can accumulate quickly if not deleted periodically. Deleting reports can be a time-consuming and tedious task. Worry-Free Business Security Advanced 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

Delete outdated reports by limiting the number reports Worry-Free Business Security Advanced stores.

Navigation Path: Reports > Maintenance > Reports tab

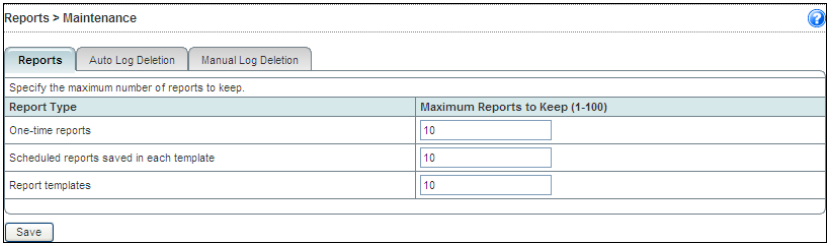


FIGURE 10-4. Reports Maintenance screen

To set the maximum number of reports to keep:

1. 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**
2. Click **Save**.

Automatically Deleting Logs

Automatically delete outdated logs by setting the maximum number of days to store logs.

Navigation Path: Reports > Maintenance > Auto Log Deletion tab

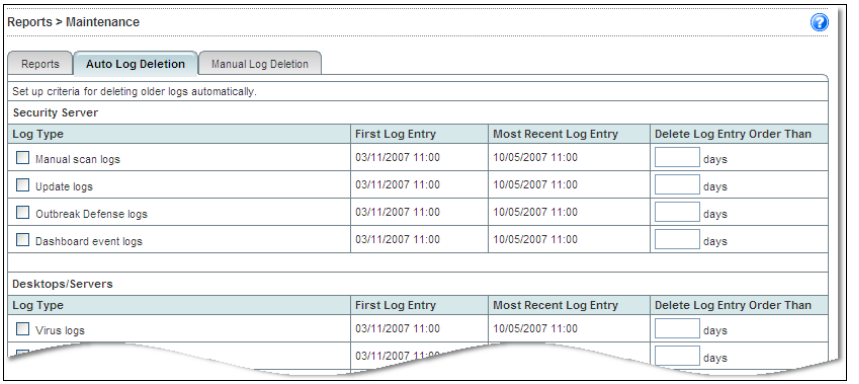


FIGURE 10-5. Auto Log Deletion screen

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 Deleting Logs

Manually delete logs when they are no longer required.

Navigation Path: Reports > Maintenance > Reports tab

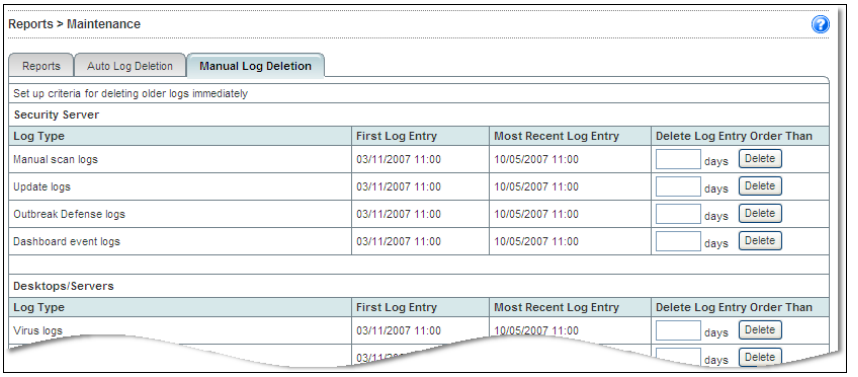


FIGURE 10-6. Manual Log Deletion screen

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** corresponding to the log type.
2. Click **Save**.

Tip: To delete all the logs, specify zero (0) as the number of days and click **Delete**.

Chapter 11

Working with Notifications

This chapter explains how to use the different notification options. The topics discussed in this chapter include:

- *About Notifications* on page 11-2
- *Configuring Notifications* on page 11-3
- *Customizing Notification Alerts* on page 11-5
- *Configuring Notification Settings* on page 11-6

About Notifications

To minimize the amount of time Administrators need to monitor Worry-Free Business Security Advanced and to ensure Administrators receive early warnings about looming outbreak situations, set the Security Server to send notifications whenever there are abnormal events on the network. Worry-Free Business Security Advanced can send notifications using email, SNMP, or Windows event logs.

The conditions for notifications affect the Live Status screen. The conditions trigger the status icon to change from Normal to Warning or to Action Required.

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

Threat Events

- **Outbreak Defense:** An alert is declared by TrendLabs or highly critical vulnerabilities are detected.
- **Antivirus:** Virus/malware detected on Clients or Microsoft Exchange servers 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 also configure the spyware/grayware notification threshold, that is, the number of spyware/grayware incidents detected within the specified time period (default is one hour).
- **Web Threat Protection:** 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.
- **Anti-spam:** Spam occurrences exceed a certain percentage of total email messages.
- **Network Virus:** Network viruses detected exceeds a certain number.

System Events

- **License:** Product license is about to expire or has expired, seat count usage is more than 80%, or seat count is usage more than 100%.
- **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.

Configuring Notifications

Configuring Notifications involves two steps — First, select the events for which you need notifications and then configure the methods of delivery. Worry-Free Business Security Advanced offers three methods for delivery — email notifications, SNMP notifications, and Windows Event log.

Navigation Path: Preferences > Notifications > Events tab

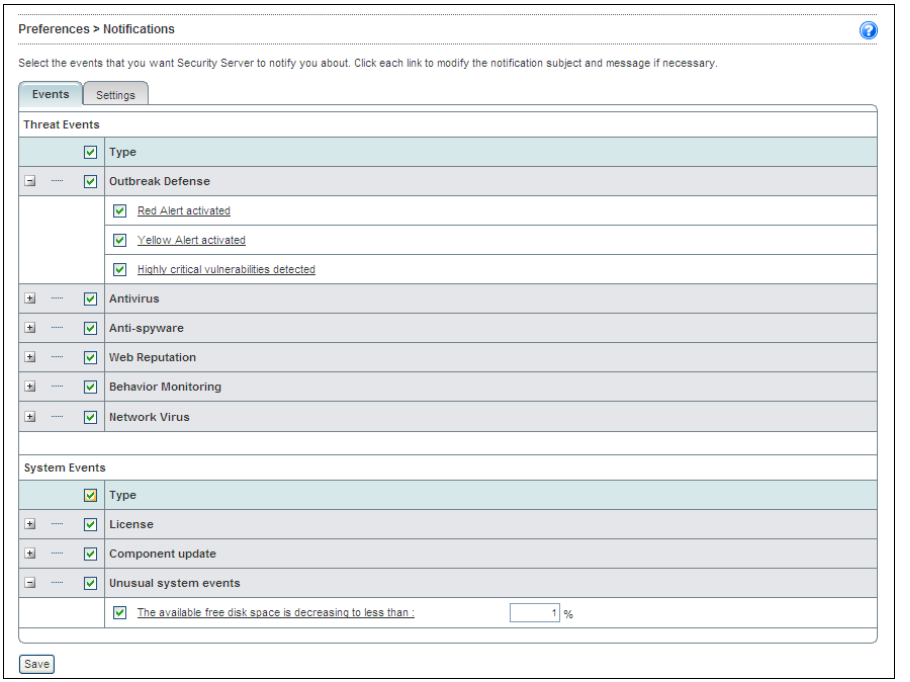


FIGURE 11-1. Notification Events screen

To configure notification events:

1. From the **Events** tab on the **Notifications** screen, update the following as required:
   - **Threat Events:** Select the **Type** check box to receive notifications for all events. Alternatively, select check boxes corresponding to individual events.
   - Click + to expand each event and configure the threshold and/or time period for the event.
2. Click **Save.**

Customizing Notification Alerts

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

Navigation Path: Preferences > Notifications > Click a notification

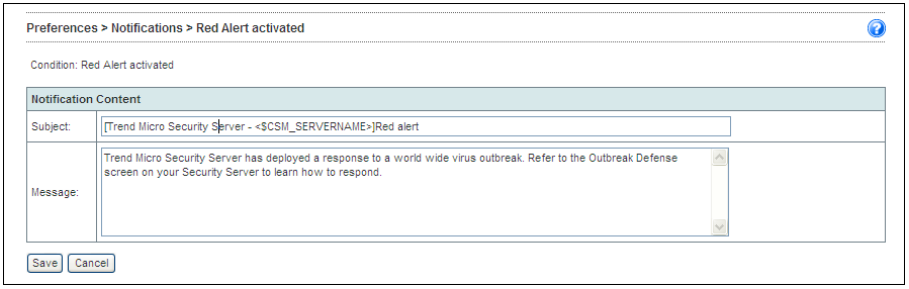


FIGURE 11-2. Notification content screen

To customize the content of a notification:

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

---

1. Type the new subject line in the **Subject** field.
2. Type the new message in the **Message** field.
3. Click **Save.**

Configuring Notification Settings

Navigation Path: Preferences > Notifications > Settings tab

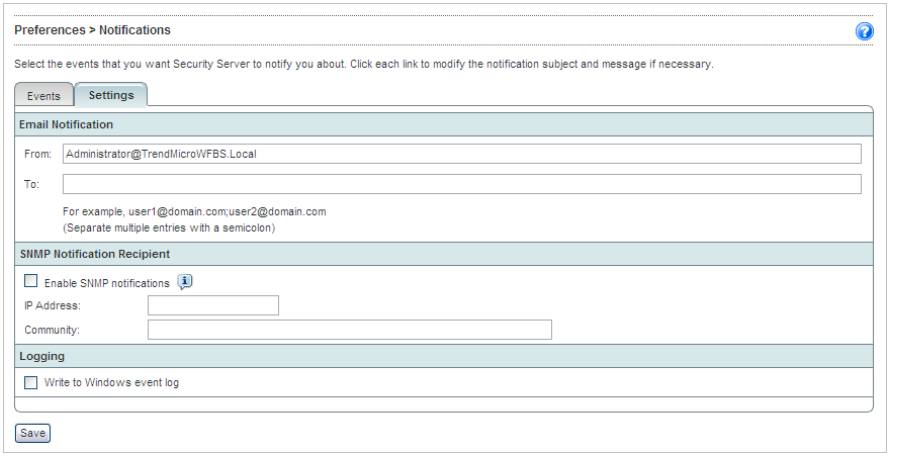


FIGURE 11-3. Notifications screen

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 of the notifications. Configure the content of the email message from the **Events** tab.
     - **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**

Note: You can use either or all of the above-mentioned notification methods.

2. Click **Save.**

Chapter 12

Configuring Global Settings

This chapter explains how to use Global Settings. The topics discussed in this chapter include:

- *Internet Proxy Options* on page 12-2
- *SMTP Server Options* on page 12-3
- *Desktop/Server Options* on page 12-3
- *System Options* on page 12-10

Internet Proxy Options

If the network uses a proxy server to connect to the Internet, specify proxy server settings for the following services:

- Component updates, license notifications, and the Smart Protection Network
  To set proxy server settings for these services, modify the fields under **Settings for updates, license notifications, and Smart Protection Network** in the **Proxy** tab.
- Web Threat Protection and Behavior Monitoring
  To set proxy server settings for these services, modify the fields under **Settings for Web Threat Protection and Behavior Monitoring** in the **Proxy** tab.

Note: Note: CSA will always use the same proxy server and port used by Internet Explorer to connect to the Internet for Web Threat Protection and behavior monitoring. 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.

Navigation Path: Preferences > Global Settings > Proxy tab

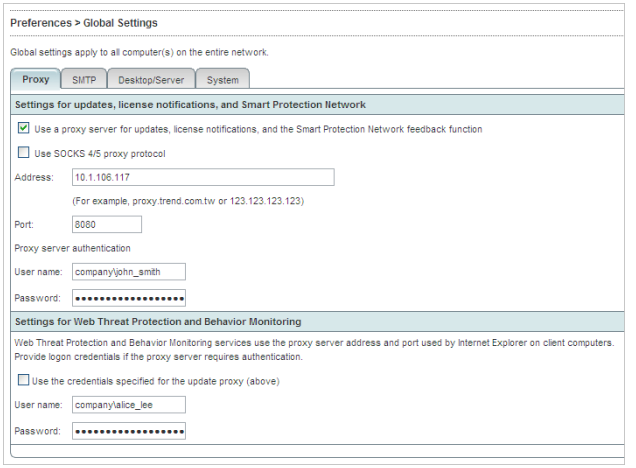


FIGURE 12-1. Global Settings–Proxy Server Settings screen

SMTP Server Options

The SMTP Server settings apply to all notifications and reports generated by Worry-Free Business Security Advanced.

Navigation Path: Preferences > Global Settings > SMTP tab

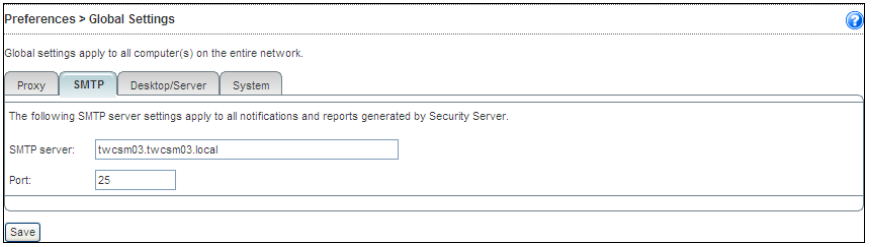


FIGURE 12-2. SMTP tab on the Global Settings screen

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 the name of the SMTP server.
   - **Port**
2. Click **Save**.

Desktop/Server Options

The Desktop/Server options pertain to the Worry-Free Business Security Advanced 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.

Navigation Path: Preferences > Global Settings > Desktop/Server tab

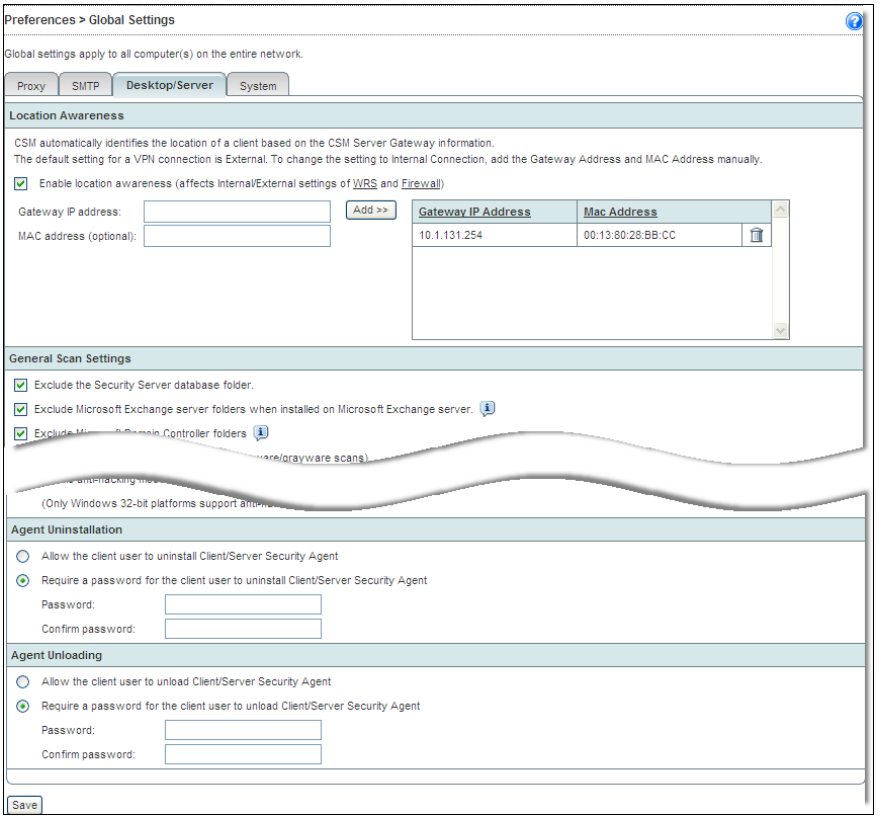


FIGURE 12-3. Desktop/Server tab of the Global Settings screen

To set the Desktop/Server options:

1. From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:
   - *Location Awareness* on page 12-5
   - *General Scan Settings* on page 12-5
   - *Virus Scan Settings* on page 12-6
   - *Spyware/Grayware Scan Settings* on page 12-7

- *Web Threat Protection* on page 12-7
- *Behavior Monitoring* on page 12-7
- *IM Content Filtering* on page 12-8
- *Alert Settings* on page 12-8
- *Watchdog Settings* on page 12-9
- *Agent Uninstallation* on page 12-9
- *Agent Unloading* on page 12-9

2. Click **Save**.

Location Awareness

Location Awareness controls the In Office/Out of Office connection settings. Refer to *Control Security Settings Based on Location* on page 1-24 for more information.

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 Web Threat Protection, TrendSecure, and Firewall.
- **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 improves security by permitting only the configured device to connect.

  Click the corresponding  icon to delete an entry.

General Scan Settings

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **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, Worry-Free Business Security Advanced 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** Client/Server Security Agent link to the context-sensitive menu. With this, users can right-click a file or folder (on the Desktop or in Windows Explorer) and manually scan the file or folder.

Spyware/Grayware Scan Settings

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

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

Web Threat Protection

Web Threat Protection enhances protection against visiting malicious Web sites. Web Threat Protection leverages Trend Micro's extensive Web security database to check the reputation of HTTP URLs that users are attempting to access or URLs that are embedded in email messages. Refer to *Protect Clients from Visiting Malicious Web Sites* on page 1-26 for more details.

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**.

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

- **Approved URL** list**:** URLs in this list will not be blocked. To delete an entry, click the corresponding  icon.
- **Enable CSA usage logs:** Agents will send details of accessed URLs to the Security Server.

Refer to *Web Threat Protection* on page 5-15 for details on configuring Web Threat Protection based on the Client's location.

Behavior Monitoring

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

Enable pop-ups for low-risk changes or actions monitored: Agents warn the users of low-risk change or monitored actions.

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:

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

From the **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  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 Client/Server Security Agent is constantly protecting Clients. When enabled, the Watchdog checks the availability of the Agent every x minutes. If the Agent is unavailable, the Watchdog will attempt to restart the Agent.

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

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

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

Agent Uninstallation

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Allow the client user to uninstall** Client/Server Security Agent**:** Allows users to uninstall the Client/Server Security Agent.
- **Require a password for the client user to uninstall** Client/Server Security Agent**:** Allows users to uninstall the Client/Server Security Agent after providing the specified password.
  - **Password**
  - **Confirm password**

Agent Unloading

From the **Desktop/Server** tab of the **Global Settings** screen, update the following as required:

- **Allow the client user to unload** Client/Server Security Agent**:** Allows users to unload the Client/Server Security Agent.
- **Require a password for the client user to unload the** Client/Server Security Agent**:** Allows users to unload the Client/Server Security Agent after providing the specified password.
  - **Password**
  - **Confirm password**

System Options

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.

Navigation Path: Preferences > Global Settings > System tab

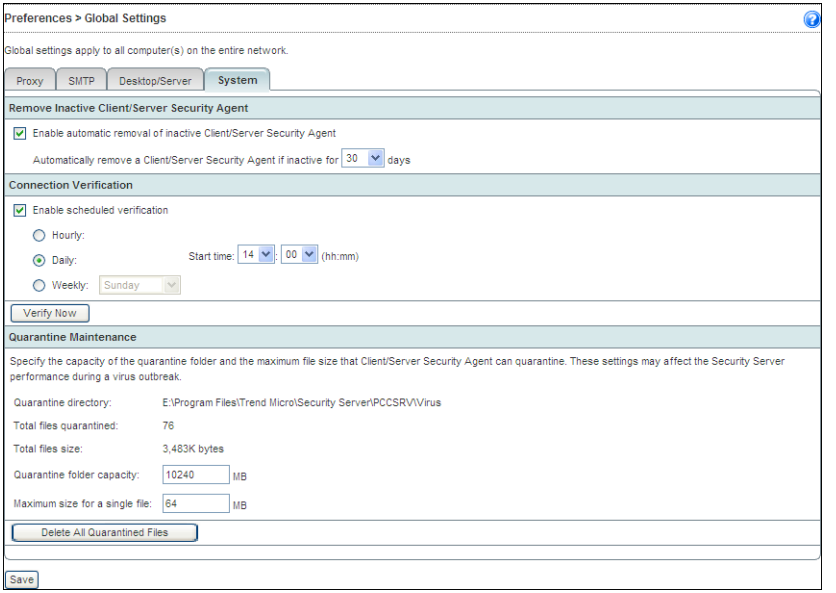


FIGURE 12-4. System tab of the Global Settings screen

To set the System options:

1. From the **System** tab of the **Global Settings** screen, update the following as required:
   - *Removing Inactive Client/Server Security Agents* on page 12-11
   - *Verifying Client-Server Connectivity* on page 12-12
   - *Maintaining the Quarantine Folder* on page 12-12
2. Click **Save**.

Removing Inactive Client/Server Security Agents

When you use the Client/Server Security Agent uninstallation program on the Client to remove the Agents from a 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 Client/Server 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 Client/Server Security Agent as inactive. If a user unloads or disables the Agent for an extended time, the Security Server also displays the Client/Server Security Agent as inactive.

To have the Security Groups Tree only display active Clients, you can configure the Security Server to remove inactive Client/Server 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** Client/Server Security Agent**:** Enables the automatic removal of Clients that have not contacted the Security Server for the specified number of days.
   - **Automatically remove a** Client/Server 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.**

Verifying Client-Server Connectivity

Worry-Free Business Security Advanced 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. Worry-Free Business Security Advanced encrypts the infected file to prevent it from infecting other files.

The default location of Client/Server Security Agent quarantine folder is as follows:

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

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 12-6.

To maintain quarantine folders:

1. From the **System** tab of the **Global Settings** screen, update the following as required:
   - **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 13

Performing Additional Administrative Tasks

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 13-5
- *Uninstalling the Trend Micro Security Server* on page 13-6

Changing the Web Console Password

To prevent unauthorized users from modifying your settings or removing the Agent from your Clients, the Web console is password protected. The Worry-Free Business Security Advanced master setup program requires you to specify a Web console password; however, you can modify your password from the Web console.

Tip: 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

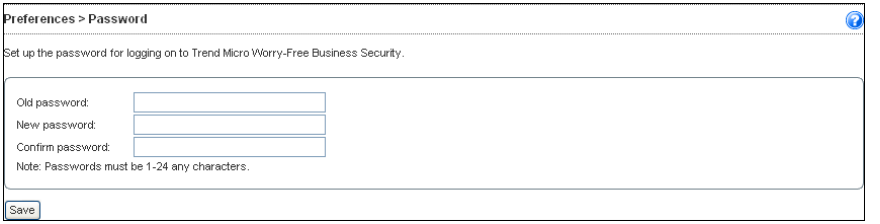


FIGURE 13-1. Preferences–Password screen

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 Worry-Free Business Security Advanced. Refer to *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 Worry-Free Business Security Advanced 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.

Refer to the Plug-in's documentation for more information.

Viewing Product License Details

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

Navigation Path: Preferences > Product License

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 download engine or pattern file updates. 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

Your participation in the Trend Micro Smart Protection Network will help Trend Micro provide proactive solutions that block threats before they reach you. As part of the Smart Protection Network, you provide important data to our correlation technologies, which are then able to weed out threat sources before they can do more harm. This feedback mechanism gathers threat information based on the reputation of the communication source, not on the content of the specific communication, so the privacy of your personal or business information is protected.

Navigation Path: Preferences > Smart Protection Network

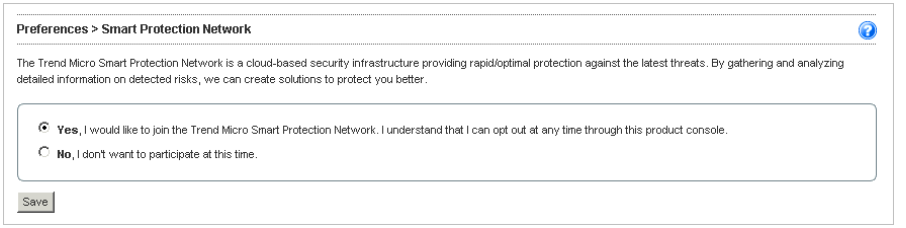


FIGURE 13-3. Smart Protection Network enrollment screen

For more information on the Smart Protection Network, visit:

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

Changing the Agent's Interface Language

Administrators can provide locale-specific language packs for Client/Server Security Agents. After administrators install all the language packs users will be able to see the Client/Server Security Agent interface in the language corresponding to operating system's locale.

Note: The language used on the Agent interface will correspond to the locale configured on the Client operating system.

To provide language packs:

1. Download the appropriate language packs from the links.
2. Copy the language packs to `PCCSRV\Download\LangPack\` on the Security Server.
3. Restart the Clients that require the new language pack.

Uninstalling the Trend Micro Security Server

WARNING! *Uninstalling Trend Micro Security Server makes your network vulnerable.*

Worry-Free Business Security Advanced 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. Refer to *Removing Agents* on page 3-21.

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.

Chapter 14

Using Administrative and Client Tools

This chapter explains how to use the Administrative and Client tools that come with Worry-Free Business Security Advanced.

The topics discussed in this chapter include:

- *Tool Types* on page 14-2
- *Administrative Tools* on page 14-3
- *Client Tools* on page 14-8
- *Add-ins* on page 14-13

Tool Types

Worry-Free Business Security Advanced 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 Trend Micro Security Server and manage Agents
  - **Login Script Setup** (`autopcc.exe`)**:** Automates Client/Server Security Agent installation.
  - **Vulnerability Scanner** (`TMVS.exe`)**:** Locates unprotected computers on the network.
- **Client tools:** Helps enhance the performance of the Agents.
  - **Client Packager** (`ClnPack.exe`)**:** Creates a self-extracting file containing the Client/Server Security Agent and components.
  - **Restore Encrypted Virus** (`VSEncode.exe`)**:** Opens infected files encrypted by Worry-Free Business Security Advanced.
  - **Touch Tool** (`TmTouch.exe`)**:** Change the time stamp on a hot fix to synchronize it with the system clock.
  - **Client Mover Tool** (`IpXfer.exe`)**:** Transfers Clients from one Security Server to another. Source and destination servers must be running the same version of Worry-Free Business Security Advanced and operating systems.
- **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 from the Live Status screen.

Note: Some tools available in previous versions of Worry-Free Business Security Advanced are not available in this version. If you require these tools, contact Trend Micro Technical Support. Refer to *Trend Micro Support* on page 15-19

Administrative Tools

This section contains information about Worry-Free Business Security Advanced administrative tools.

Login Script Setup

With Login Script Setup, you can automate the installation of the Client/Server 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 Client/Server Security Agent
- Updates the virus pattern file and program files

For instructions on installing Agents, refer to *Installing with Login Script Setup* on page 3-7.

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 Client/Server Security Agent remotely on computers running Windows Vista/2000/XP (Professional only)/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 Client/Server Security Agent with Vulnerability Scanner if the server component of Worry-Free Business Security Advanced is **present** on the same machine.
Vulnerability Scanner does not install the Client/Server Security Agent on a machine already **running** the server component of Worry-Free Business Security Advanced.

To configure Vulnerability Scanner:

1. In the drive where you installed the server component of Worry-Free Business Security Advanced, 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 only supports class B 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 14-4.

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`.

Client Tools

This section contains information about Worry-Free Business Security Advanced 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. It also includes an email function that can access your Microsoft Outlook address book and allow you to send the self-extracting file from within the tool's console.

To run Client Packager, double-click the file. Worry-Free Business Security Advanced Clients that are installed using Client Packager report to the server where the setup package was created.

Restore Encrypted Virus

Client/Server 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 Client/Server 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 Client/Server Security Agent 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

To decrypt files in the quarantine folder:

1. Copy `VSEncrypt` from the Security Server to the Client:

   `\PCCSRV\Admin\Utility\VSEncrypt`.

WARNING! *Do not copy the* `VSEncrypt` *folder to the Worry-Free Business Security Advanced 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. Refer to

Touch Tool

The Touch Tool synchronizes the time stamp of one file with the time stamp of another file or with the system time of the computer. If you are unsuccessful in deploying a hot fix (an update or patch that Trend Micro releases) on the Trend Micro

Security Server, use the Touch Tool to change the time stamp of the hot fix. This causes Worry-Free Business Security Advanced to interpret the hot fix file as new, which makes the server attempt to deploy the hot fix again automatically.

To run the Touch Tool:

1. On the Trend Micro Security Server, go to the following directory:

   `\PCCSRV\Admin\Utility\Touch`

2. Copy the `TmTouch.exe` file to the folder where the file you want to change is located. If synchronizing the file time stamp with the time stamp of another file, put both files in the same location with the Touch tool.
3. Open a command prompt and go to the location of the Touch Tool.
4. Type the following:

   `TmTouch.exe <destination_filename> <source_filename>`

   where:

   `<destination_filename>` = the name of the file (the hot fix, for example) whose time stamp you want to change

   `<source_filename>` = the name of the file whose time stamp you want to replicate

   If you do not specify a source filename, the tool sets the destination file time stamp to the system time of the computer.

Note: You can use the wildcard character "*" in the destination file name field, but not the source file name field.

5. To verify the time stamp changed, type `dir` in the command prompt or right click the file in Windows explorer and select **Properties**.

Client Mover

If you have more than one Worry-Free Business Security Advanced server on the network, you can use Client Mover to transfer Clients from one Worry-Free Business Security Advanced server to another.

This is especially useful after adding a new Worry-Free Business Security Advanced 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 Worry-Free Business Security Advanced and operating systems.

Client Mover requires the `IpXfer.exe` file.

To run Client Mover:

1. On the Worry-Free Business Security Advanced 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:

   - `<server_name>` = the server name of the destination Worry-Free Business Security Advanced server (the server to which the Client will transfer)
   - `<server_listening_port>` = the listening (trusted) port of the destination Worry-Free Business Security Advanced server. To view the listening port on the Web console, click **Security Settings**. The listening port is shown next to the Security Server name.
   - `1` = You must use the number "1" after "-m"
   - `<client_listening_port>` = the port number of the Client

To confirm that the Client now reports to the other server:

1. On the Client, right click the Client/Server Security Agent icon in the system tray.
2. Select Client/Server Security Agent **Console**.
3. From the **Help** tab, click **more info** in the **Product Information** section.
4. Verify that the Security Server that the CSA reports to is correct.

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.

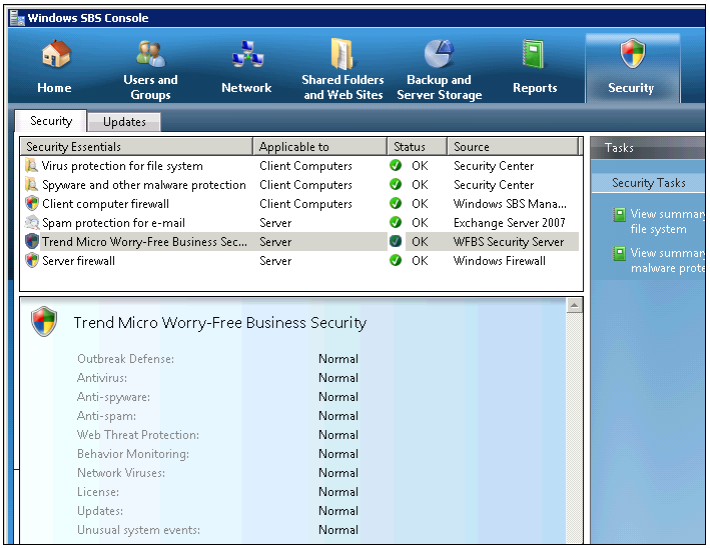


FIGURE 14-1. SBS console displaying live status information

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 > 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.

Using the SBS and EBS Add-ins

The SBS and EBS add-ins let administrators view high-level security and system status information on 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.

Chapter 15

FAQs, Troubleshooting, and Technical Support

This chapter provides answers to commonly asked questions about installation and deployment, describes how to troubleshoot problems that may arise with Worry-Free Business Security Advanced, and provides information you will need to contact Trend Micro technical support. The topics discussed in this chapter include:

- *Frequently Asked Questions (FAQs)* on page 15-2
- *Troubleshooting* on page 15-7
- *Trend Micro Security Information Center* on page 15-18
- *Known Issues* on page 15-19
- *Contacting Trend Micro* on page 15-19
- *Trend Micro Support* on page 15-19
- *About TrendLabs* on page 15-22
- *About Trend Micro* on page 15-22

Frequently Asked Questions (FAQs)

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

How can I further protect Clients?

You can take many steps to prevent the installation of spyware/grayware onto your Clients. Trend Micro suggests making the following standard practices part of the security initiative in your organization:

- Follow all Trend Micro recommendations in this document.
- Educate your 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 users are certain both the creator of the software and the Web site they are viewing are trustworthy.
  - Disregard unsolicited commercial email (spam), especially if the spam asks users to click a button or hyperlink.
- Configure Web browser settings that ensure a strict level of security. Trend Micro recommends requiring Web browsers to prompt users before installing ActiveX controls. To increase the security level for Internet Explorer (IE), go to **Tools** > **Internet Options** > **Security** and move the slider to a higher level. If this setting causes problems with Web sites you want to visit, click **Sites**, and add the sites you want to visit to the trusted sites list.
- If using Microsoft Outlook, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages. Creators of spyware/grayware often use pictures.
- Prohibit the use of peer-to-peer file-sharing services. Spyware/grayware applications may be masked as other types of files your users may want to download, such as codecs, MP3s, plug-ins, and so on.
- Periodically examine the installed software on Clients and look for applications that may be spyware/grayware. If you find an application or file that Worry-Free Business Security Advanced cannot detect as grayware but you think is a type of grayware, send it to Trend Micro:
  http://subwiz.trendmicro.com/SubWiz

Trend Micro will analyze the files and applications you submit.

If you prefer to communicate through email, send a message to the following address:

virusresponse@trendmicro.com

See *Contacting Technical Support* on page 15-20 for more information.

- Keep your Windows operating systems updated with the latest patches and updates from Microsoft. See the Microsoft Web site for details.
- **Regarding protection for offline Clients:** Clients that could not connect to the Security Server, called *offline Clients*, benefit from continuous protection provided by the CSA. However, these Clients may be unable to connect to update sources in your network. To allow Clients to update when offline, ensure that they have the privilege to connect to the Trend Micro ActiveUpdate server. Clients with this privilege connect to the Trend micro server automatically when other update sources are unavailable. For more information on client privileges, see *Configuring Client Privileges* on page 5-26.

Registration

I have several questions on registering Worry-Free Business Security Advanced. Where can I find the answers?

See the following Web site for frequently asked questions about registration:

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

Installation, Upgrade, and Compatibility

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

Refer to the Trend Micro™ Worry-Free™ Business Security Advanced *Getting Started Guide* for information.

Which Agent installation method is best for my network environment?

Refer to *Choosing an Installation Method* 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 Worry-Free Business Security Advanced support 64-bit platforms?

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

Can I upgrade to Worry-Free Business Security Advanced from Trend Micro™ ServerProtect?

No. ServerProtect will have to be first uninstalled and then Worry-Free Business Security Advanced can be installed.

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 display 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 Worry-Free Business Security Advanced settings. Where can I find the answers?

You can download all Worry-Free Business Security Advanced documentation from the following site:

http://www.trendmicro.com/download

What exclusions should I use for Antivirus software with SBS 2003?

Refer to the following tables for the SBS 2003 exclusions:

TABLE 15-1. Microsoft Exchange exclusions

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

TABLE 15-2. IIS exclusions

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

TABLE 15-3. Domain controller exclusions

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

TABLE 15-4. Windows SharePoint services exclusions

Temporary SharePoint folder	C:\windows\temp\FrontPageTempDir

TABLE 15-5. Client Desktop folder exclusions

Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore

TABLE 15-6. 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

Documentation

What documentation is available with this version of Worry-Free Business Security Advanced?

This version of Worry-Free Business Security Advanced includes the following: *Administrator's Guide, Getting Started Guide*, readme file, and help files for the Web console, Master Installer, and Client/Server Security Agent.

Can I download the Worry-Free Business Security Advanced documentation?

Yes. You can download the Administrator's Guide, Getting Started Guide, and readme file from the following site:

http://www.trendmicro.com/download

I have questions/issues with the documentation. How can I provide feedback to Trend Micro?

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

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

Troubleshooting

This section helps you troubleshoot issues that may arise while using Worry-Free Business Security Advanced.

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 (*Client Packager* on page 14-8).
2. Manually install the package on the computer.

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

If Agents cannot access the Security Server:

1. Create a new package using the Client Packager (*Client Packager* on page 14-8).
2. Manually install the package on the computer.

The Client is protected but does not receive updates from the Security Server.

User's Spam Folder not Created

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

- An end user logs on to their mailbox for the first time

- The first email arrives at the mailbox

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

Internal Sender/Recipient Confusion

You can only define one domain as the internal address for the Messaging Security Agent. If you use Microsoft Exchange System Manager to change your primary address on a server, Messaging Security Agent does not recognize the new address as an internal address because Messaging Security Agent cannot detect that the recipient policy has changed. To update the Internal Email Definition, refer to *Notification Settings* on page 6-50.

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

Re-sending a Quarantine Message Fails

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

To resolve quarantined message failure:

1. Using the Windows Registry Editor, open the following registry entry on the server:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion
   ```

2. Edit the entry as follows:

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

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

3. Close the Registry Editor.

Replicating Settings Fails

You can only replicate settings from a source Messaging Security Agent to a target Messaging Security Agent that share the same domain. Messaging Security Agent is unable to replicate settings when the source Messaging Security Agent is located in the parent domain, and the target Messaging Security Agents is located in the child domain (or vice versa), because it lacks the required permission.

To solve this problem, perform the following:

For Windows 2003 operating system:

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

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

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

For Windows 2000 operating system:

1. Start **regedt32.**
2. Go to

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

3. Click **winreg.**
4. Select **winreg > Security > Permissions.**
5. Add **Smex Admin Group** of target domain, and enable **Allow Read.**

6. Go to

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

7. Click **ScanMail for Microsoft Exchange.**
8. Select **Security > Permissions**.
9. Add **Smex Admin Group** of target domain, and enable **Allow Read** and **Allow Full Control.**

Messaging Security Agents and Source Location

If the source and target Messaging Security Agents are located in different forests, there will be no way to replicate the settings to the selected target Messaging Security Agents.

MSA SQL Server® Dependency in Exchange Server 2007

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

- **ScanMail_Master**
- **ScanMail_RemoteConfig**

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

Saving and Restoring Program Settings for Rollback or Reinstallation

You can save a copy of the Worry-Free Business Security Advanced database and important configuration files for rolling back your Worry-Free Business Security Advanced program. You may want to do this if you are experiencing problems and want to reinstall Worry-Free Business Security Advanced 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 Worry-Free Business Security Advanced quarantines infected files.
   - **`HTTDB` folder:** Contains the Worry-Free Business Security Advanced database.
3. Uninstall Worry-Free Business Security Advanced (see *Uninstalling the Trend Micro Security Server* on page 13-6).
4. Perform a fresh install. Refer to the Trend Micro™ Worry-Free™ Business Security Advanced *Getting Started Guide*.
5. After the master installer finishes, stop the Trend Micro Security Server Master Service on the target computer.
6. Update the virus pattern version from the backup file:

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

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

   ComponentName=Virus pattern
   ```

```
Version=xxxxxx 0 0
```

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

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

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

---

7. With the backups you created, overwrite the Worry-Free Business Security Advanced 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 Worry-Free Business Security Advanced, 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. For more information on the Verify Connection feature, refer to *Verifying Client-Server Connectivity* on page 12-12.

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.

To verify unsuccessful installations:

- 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 if the proxy settings are configured correctly.
- Delete Trend Micro add-ons and browsing history.

  a. Close and re-open Internet Explorer.

  b. In Internet Explorer, click **Tools > Internet Options.** The **Internet Options** screen appears.

  c. In the **Browsing History** section, click **Delete.** The **Delete Browsing History** screen appears.

  d. Click **Delete All.** Confirm to delete files and settings stored by add-ons.

  e. In the **Programs** tab, click **Manage add-ons.** The Manage Add-ons screen appears.

  f. Select and delete all Trend Micro add-ons for all categories in the Show drop-down list box.

  Tip: Sort entries by Publisher to group Trend Micro add-ons.

  g. Close the windows and restart Internet Explorer.

h. Start the installation. Refer to *Installing from an Internal Web Page* on page 3-6 or *Installing with Remote Install* on page 3-12 for additional instructions.

- Open a Web browser on the Client, and type `https://{Server name}:{server port} /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 you have Administrator privileges to the target computer where you want to install the Agent.
- Check if the target computer meets the minimum system requirements.
- Check if any files have been locked.
- If you have limited bandwidth, check if it causes connection timeout between the server and the Client.

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

```
Uninstallation failed.
```

There are several possible causes for this error:

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

There are also several possible solutions for this error:

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

To manually remove third-party software:

- If the third-party software is registered to the Add/Remove Programs
  - **a.** Open the Control Panel.
  - **b.** Double-click **Add/Remove Programs**.
  - **c.** Select the third-party software from the list of installed programs.
  - **d.** Click **Remove**. Follow the on-screen instructions.
- If the third-party software is not registered to the Add/Remove Programs
  - **a.** Open the Windows registry.
  - **b.** Go to `HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Uninstall`.

c. Locate the third-party software and run the uninstall string value.

- If the third-party software's setup program is in MSI format:

  a. Locate the product number

  b. Verify the product number

  c. Run the uninstall string

> **Note:** Some product uninstallation keys are in the Product Key folder and you might have to delete them manually.

To modify the startup of the service for the third-party software:

1. Restart the computer in Safe mode.
2. Modify the service startup from automatic to manual.
3. Restart the system again.
4. Manually remove the third-party software.

To unload the service or process for the third-party software:

> **WARNING!** *This procedure may cause undesirable effects to your computer if performed incorrectly. Trend Micro recommends backing up your system first.*

1. Unload the service for the third-party software.
2. Open the Windows registry, then locate and delete the product key.
3. Locate and delete the **Run** or **Run service** key.
4. Verify that the service registry key in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` has been removed.

Invalid/Expired Digital Signatures

In the event of a program's digital signature expiring, administrators would need to update the signature. Refer to the following link to update digital signatures:

http://technet.microsoft.com/en-us/library/bb457160.aspx

Or, contact the vendor of the program.

Trend Micro Security Information Center

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

http://www.trendmicro.com/vinfo

Visit the Security Information site to:

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

Known Issues

Known issues are features in Worry-Free Business Security Advanced 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.

Contacting Trend Micro

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

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

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

Trend Micro Support

Trend Micro Support can help you resolve queries relating to your Trend Micro products. Most queries have already been answered on the Knowledge Base (refer *Knowledge Base* on page 15-20 for more information). If you cannot find your answer on the Knowledge Base, you can contact Trend Micro Technical Support for further assistance (refer *Contacting Technical Support* on page 15-20 for more information).

Knowledge Base

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

Also available in the Knowledge Base are product FAQs, tips, advice on preventing virus/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

Contacting 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 15-21) 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 15-21.
   - Visit the following URL:

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

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

- If you prefer to communicate by email message, send a query to the following address:

virusresponse@trendmicro.com

- In the United States, you can also call the following toll-free telephone number:

(877) TRENDAV, or 877-873-6328

Using the Case Diagnostic Tool

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

Download the Case Diagnostic Tool from:

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

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.

About TrendLabs

TrendLabs is Trend Micro's 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.

About Trend Micro

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

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impact of threats to information by offering centrally controlled, server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro enables companies and service providers worldwide to stop virus/malware and other malicious code from a central point, before they ever reach the desktop.

To make this possible, TrendLabs, a global network of antivirus research and product support centers, provides continuous 24 x 7 coverage to Trend Micro customers

around the world. TrendLabs' modern headquarters has earned ISO 9002 certification for its quality management procedures—one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

Trend Micro is headquartered in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia—a global organization with more than 3,000 employees in 25 countries.

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

http://www.trendmicro.com

Appendix A

System Checklists

Use the checklists in this appendix to record relevant system information as a reference.

Ports Checklist

Worry-Free Business Security Advanced uses the following default ports.

TABLE 1-1. Port Checklist

PORT	SAMPLE	YOUR VALUE
SMTP	25	
Proxy	Administrator Defined	
Security Server	8059	
Web console	4343	
Trend Micro Security Server	8080	
Client/Server Security Agent	21112	
Messaging Security Agent	16372	

Server Address Checklist

Worry-Free Business Security Advanced requires the following information during installation and during configuration. Record these details for easy reference.

TABLE 1-2. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Trend Micro Security Server information		
IP address	192.168.1.1	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Web server information		
IP address	192.168.1.1	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Proxy server for component download		
IP address	192.168.1.1	
Fully Qualified Domain Name (FQDN)	proxy.company.com	
NetBIOS (host) name	proxyserver	
SMTP server information (Optional; for email notifications)		
IP address	192.168.1.1	
Fully Qualified Domain Name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	

TABLE 1-2. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
SNMP Trap information (Optional; for SNMP Trap notifications)		
Community name	company	
IP address	192.168.1.1	

Appendix B

Trend Micro Product Exclusion List

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

TABLE 2-1. Trend Micro product exclusion list

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

TABLE 2-1. Trend Micro product exclusion list

Product Name	Installation Path Location
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion ProgramDirectory={Installation Drive}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion ProgramDirectory=
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro \IM Security\CurrentVersion HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro \ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro \ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro \ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder=

TABLE 2-1. Trend Micro product exclusion list

Product Name	Installation Path Location
ScanMail for Microsoft Exchange (SMEX) Continued	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= i Get exclusion.txt file path from HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir ii Go to HomeDir path (for example, C:\Program Files\Trend Micro\Messaging Security Agent\) iii 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

By default, when the Client/Server 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\CurrentVersi
on\Misc.

ExcludeMicrosoftExchangeStoreFiles=C:\Program
Files\Exchsrvr\mdbdata\priv1.stm|C:\Program
Files\Exchsrvr\mdbdata\priv1.edb|C:\Program
Files\Exchsrvr\mdbdata\pub1.stm|C:\Program
Files\Exchsrvr\mdbdata\pub1.edb

ExcludeMicrosoftExchangeStoreFolders=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. For more information, refer to:

http://support.microsoft.com/kb/245822/

Appendix C

Trend Micro Services

The topics discussed in this chapter include:

- *Trend Micro Outbreak Prevention Policy* on page C-2
- *Trend Micro Damage Cleanup Services* on page C-2
- *Trend Micro Vulnerability Assessment* on page C-3
- *Trend Micro IntelliScan* on page C-4
- *Trend Micro ActiveAction* on page C-4
- *Trend Micro IntelliTrap* on page C-6
- *Trend Micro Email Reputation Services* on page C-7
- *Trend Micro Web Threat Protection* on page C-7

Trend Micro Outbreak Prevention Policy

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

The Outbreak Prevention Policy is downloaded from Trend Micro to the 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
- Displays an alert message on Clients when an outbreak detected

Trend Micro Damage Cleanup Services

Worry-Free Business Security Advanced 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:

- **Virus Cleanup Engine:** The engine Damage Cleanup Services uses to scan for and remove threats and its associated processes.
- **Virus Cleanup Template:** Used by the Virus Cleanup Engine, this template helps identify threats and its associated processes so the engine can eliminate them.

In Worry-Free Business Security Advanced, DCS runs on the Client on these occasions:

- Users perform a manual cleanup from the Agent console.
- Administrators perform Cleanup Now on the Client from the Web console.
- Users run Manual or Scheduled Scan.
- After hot fix or patch deployment (see for more information).
- When the Worry-Free Business Security Advanced service is restarted (the Worry-Free Business Security Advanced Client Watchdog service must be selected to restart the Agent automatically if the Agent unexpectedly terminates. Enable this feature on the **Global Client Settings** screen. Refer to *Watchdog Settings* on page 12-9 for details.).

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, Worry-Free Business Security Advanced may sometimes notify the user to restart their Client to complete the process of removing threats.

Trend Micro 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.

- 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.

Trend Micro IntelliScan

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

Using IntelliScan provides the following benefits:

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

Trend Micro ActiveAction

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

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

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

Using ActiveAction provides the following benefits:

- **Time saving and easy to maintain:** ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- **Updateable 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 3-1. Default ActiveAction Settings

Threat	Action	Action for Uncleanable Threats
Possible virus/malware	No action	Not Applicable
Joke	Quarantine	Not Applicable
Other Threats	Clean	Quarantine
Packer	Quarantine	Not Applicable
Test virus	Pass	Not Applicable
Virus	Clean	Quarantine
Worm/Trojans	Quarantine	Not Applicable

Note: Future pattern files could update the default actions.

Trend Micro IntelliTrap

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

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

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

True File Type

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

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

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

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

Trend Micro Email Reputation Services

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.

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.

Trend Micro Web Threat Protection

Web Threat Protection 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 Threat Protection blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list. For information on adding a URL to the Approved URL list, refer to *Web Threat Protection* on page 12-7 for more details.

Appendix D

Client Information

Worry-Free Business Security Advanced differentiates Clients according to the following:

- Normal or Roaming Clients
- 32-bit or 64-bit Clients

Normal Clients are computers that have the Client/Server Security Agent installed and are stationary computers that maintain a continuous network connection with the Trend Micro Security Server.

Icons that appear in a Client's system tray indicate the status of the Normal Client. Refer to Table 4-1 for a list of icons that appear on the Normal Client.

TABLE 4-1. Icons that appear on a Normal Client

Icon	Description	Real-time Scan
	Normal Client	Enabled
	Pattern file is outdated	Enabled
	Scan Now, Manual Scan, or Scheduled Scan is running	Enabled
	Real-time Scan is disabled	Disabled

TABLE 4-1. Icons that appear on a Normal Client

Icon	Description	Real-time Scan
	Real-time Scan is disabled and the pattern file is outdated	Disabled
	Real-time Scan Service is not running (red icon)	Disabled
	Real-time Scan Service is not running and the pattern file is outdated (red icon)	Disabled
	Disconnected from the server	Enabled
	Disconnected from the server and the pattern file is outdated	Enabled
	Disconnected from the server and Real-time Scan is disabled	Disabled

Roaming Clients

Administrators can assign roaming mode privileges to Clients, allowing users to place these Clients into roaming mode. Clients in roaming mode, called *roaming clients*, are still protected; however, they do not receive messages from the server and are only able to update in the following circumstances:

- When the user performs Update Now or performs a Scheduled Update.
- When the Agent connects to the Trend Micro Security Server.

If you use a computer for functions that should not be interrupted by server commands, ensure that you give the CSA on that computer roaming mode privileges.

For more information on how to change client privileges, see *Client Privileges* on page 5-25.

The status of a Roaming Client is indicated by icons that appear in its system tray. Refer to Table 4-2 for a list of icons that appear on Roaming Clients.

TABLE 4-2. Icons that appear on a Roaming Client

Icon	Description	Real-time Scan
	Roaming Client (blue icon)	Enabled
	Real-time Scan is disabled	Disabled
	Pattern file is outdated	Enabled
	Real-time Scan is disabled and the pattern file is outdated	Disabled
	Real-time Scan Service is not running (red icon)	Disabled
	Real-time Scan Service is not running and the pattern file is outdated (red icon)	Disabled

32-bit and 64-bit Clients

The Client/Server Security Agent supports Windows Vista/XP/Server 2003 computers that use x86 processor architecture and x64 processor architecture. Table 4-3 shows a comparison between Worry-Free Business Security Advanced features for 32-bit and 64-bit Clients:

TABLE 4-3. 32-bit and 64-bit Client Features Comparison

Feature	32-bit Clients	64-bit Clients	Vista 32-bit Clients	Vista 64-bit Clients
Manual, Real-time, and Scheduled Scan for virus/malware and other threats	✔	✔	✔	✔
Roaming mode	✔	✔	✔	✔
Damage Cleanup Services	✔	✔	✔	✔

TABLE 4-3. 32-bit and 64-bit Client Features Comparison

Feature	32-bit Clients	64-bit Clients	Vista 32-bit Clients	Vista 64-bit Clients
Anti-spyware	✓	✓	✓	✓
Firewall	✓	✓	✓	✓
POP3 Mail Scan	✓	✓	✓	✓
Outbreak Prevention Policy	✓	✓	✓	✓
Watchdog	✓	✓	✓	✓
Manual Scan from the Windows shortcut menu	✓	✓	✓	✓
Anti-Rootkit	✓	N/A	✓	N/A
Client/Server Security Agent installation using login scripts	✓	✓	✓	✓

Note: Client/Server Security Agent does not support the Itanium 2 Architecture (IA-64).

Spyware/Grayware Types

The Trend Micro anti-spam engine can detect 21 types of spyware/grayware. The following table identifies these spyware/grayware types and provides a threat description for each type. These spyware/grayware types may appear in the **Spyware/Grayware Type** column on the **Spyware/Grayware Log Details** screen.

Spyware/Grayware Type	Threat Description
Adware	Adware is a type of software that displays advertisements on the computer screen. Typically, adware is built into software that performs some other primary task such as file sharing. The justification for adware is for the software developer to recover revenue through advertising instead of, for instance, charging for their software. Some Adware will collect the computers usage information (for example, sites visited) and send it up to a remote server on the Internet where it is collected and processed for marketing purposes.
Browser Helper Object	A type of module that acts as a plugin to a browser. Some browser helper objects may monitor or manipulate your browsing experience.
Browser Hijacker	A type of software that changes settings in your Web browser. This often includes changing your browser's default home page.

Spyware/Grayware Type	Threat Description
Cookie	Cookies are small files that are created when you visit sites on the Internet. Typically, they are used as a convenience to remember frequently used information that is required for access to a particular Web site. They can also be used to track your visits to certain Web sites and can provide companies with information about frequency of visits and other profile information. The user is usually not aware that their surfing habits are being tracked. Trend Micro Anti-Spyware identifies cookies that are created by the most common advertising companies and allows you to clean them, which helps to ensure your privacy while surfing.
CoolWebSearch Variant	A particularly complex set of Browser Hijacker variants.
Dialer	A program that usually configures some sort of dial up configuration such as a dial-up-networking connection in Windows. The user either knowingly or unknowingly will end up using the dialer that calls a time-charged number that is usually billed to your credit card.
Downloader	Software that manages the download of malicious software onto computers.
EULAware	Software that contains a non-standard or questionable End User License Agreement. For example, a license agreement that states the software or license may be updated without first notifying the user and that the user agrees to any future changes made to the software and/or license agreement. EULAware may broadly permit the software to transmit any type of information to a server, including information unrelated to the function of the software application.
General	The threat type is not known, or is not yet classified.
Keylogger/ Monitoring Software	A type of software can be either commercially sold or may be installed inadvertently through the Internet. This software can allow people to monitor your keystrokes, your computer screen, and other personal actions.
Layered Service Provider	A type of module that acts as a plugin to your Network System. LSPs usually have low level access to your network and Internet data.
Parasite	A type of software that piggybacks onto other software. This type of software may be installed without the user's knowledge or consent.
Peer To Peer	Software that allows users to exchange shared files over the Internet. Some of the files could be malicious.
Security Weakness	A medium/high risk security weakness that exists on your computer that could be used to compromise your systems security.

Spyware/Grayware Type	Threat Description
Suspect	This item is suspect, because Trend Micro Anti-Spyware detected some characteristics that match a known spyware/grayware.
Trackware	Trackware is a generic term that describes software that collects a computers demographic and usage information and sends it to some remote server through the Internet, where it can be used by other people in a variety of different ways including marketing.
Trojan	A type of software that is installed unknowingly, usually as a result of installing some other software, or viewing an email. Since it exists as a software program on the computer, the range of activity of a Trojan can be quite broad, from usage monitoring to remote control to customized collection and theft of information.
URL Shortcut	A shortcut to a malicious Web site that exists in your Internet browser or your desktop.
Virus/malware	Software that propagates itself by attaching to other valid programs, or by existing as a separate program.
Worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often through email. A worm can also be called a network virus.

Appendix F

Glossary of Terms

The following is a list of terms in this document:

Term	Description
ActiveUpdate	Connected to the Trend Micro update Web site, ActiveUpdate provides 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.
ActiveX malicious code	A type of virus that resides in Web pages that execute ActiveX controls.
Administrator	The person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
Administrator account	A user name and password that has Administrator-level privileges.
Anti-spam	Refers to a filtering mechanism, designed to identify and prevent delivery of advertisements, pornography, and other “nuisance” mail.
attachment	A file attached to (sent with) an email message.
body (message body)	The content of an email message.

Term	Description
boot sector virus	A sector is a designated portion of a disk (the physical device on which data is written and read). The boot sector contains the data used by your computer to load and initialize the computer's operating system. A boot sector virus infects the boot sector of a partition or a disk.
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.
clean	To remove virus code from a file or message.
Cleanup	Cleanup detects and removes Trojans and applications or processes installed by Trojans. It repairs files modified by Trojans.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture. Note that the online help uses the term "Client" in a special way to refer to computers that form a client-server relationship to the Worry-Free Business Security Advanced main program, the Security Server.
Clients	Clients are Microsoft Exchange servers, desktops, portable computers, and servers where a Messaging Security Agent or a Client/Server Security Agent is installed.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
COM and EXE file infectors	A type of virus that masquerades as an application by using a .exe or .com file extension.
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.
content violation	An event that has triggered the content filtering policy.
default	A value that pre-populates a field in the Web console. A default value represents a logical choice and is provided for convenience. Use default values as preset by Trend Micro or customize them as required.
Denial of Service Attack (DoS Attack)	An attack on a computer or network that causes a loss of 'service', namely a network connection. Typically, DoS attacks negatively affect network bandwidth or overload computer resources, such as memory.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, example.com. A domain name should be sufficient to determine the unique IP address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).

Term	Description
Dynamic Host Control Protocol (DHCP)	A device, such as a computer or switch, must have an IP address to be connected to a network, but the address does not have to be static. A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network.
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. Agents cannot scan encrypted files. Real-Time Scan will scan the encrypted or password protected file when it is decrypted.
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.
Exceptions	Exceptions, in relation to the Firewall, are a list of ports and communication protocols that will not be blocked by the Firewall. Exceptions also describe the ports that you have set so that they are never blocked during Outbreak Defense protection measures.
false positives	A false positive occurs when a Web site, email message, URL, or “infected” file is incorrectly determined by filtering software to be of an unwanted type. For example, a legitimate email between colleagues may be detected as spam if a job-seeking filter does not distinguish between resume (to start again) and résumé (a summary of work experience).
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
File Transfer Protocol (FTP)	FTP is a standard protocol used for transporting files from a server to a client.
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
firewall	Firewalls create a barrier between the Internet and your local network to protect the local network from hacker attacks and network virus. Firewalls examine data packet to determine if they are infected with a network virus.

Term	Description
Fully Qualified Domain Name (FQDN)	An FQDN consists of a host and domain name, including top-level domain. For example, www.trendmicro.com is a fully qualified domain name: www is the host, trendmicro is the second-level domain, and .com is the top-level domain.
grayware	Files and programs, other than virus/malware, that can negatively affect the performance of the computers on your network. These include spyware/grayware, adware, dialers, joke programs, hacking tools, remote access tools, password cracking applications, and others. The Worry-Free Business Security Advanced scan engine scans for grayware as well as virus/malware.
hot fixes and patches	Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the Worry-Free Business Security Advanced server and/or Agents.
Hyper Text Transfer Protocol (HTTP)	HTTP is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet.
HTTPS	Hypertext Transfer Protocol using Secure Socket Layer (SSL).
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet Protocol (IP)	Internet Protocol is a standardized method of transporting information across the Internet in packets of data. It is often linked to Transmission Control Protocol, which assembles the packets once they have been delivered to the intended location.
Intrusion Detection System (IDS)	Intrusion Detection Systems are commonly part of firewalls. An IDS can help identify patterns in network packets that may indicate an attack on a Client.
keywords	The Messaging Security Agent can filter incoming email messages for keywords that you set up using Content Filtering rules. When keywords are detected, the Messaging Security Agent can take action to prevent the delivery of messages containing these keywords. Note that keywords are not strictly words, but can be numbers, special characters, or short phrases.
local	The term "local" refers to a computer on which you are directly installing or running software, as opposed to a "remote" computer which is physically distant and/or connected to your computer through a network.
macro virus	A type of virus encoded in an application macro and often included in a document.

Term	Description
malware	A malware is a program that performs unexpected or unauthorized actions. It is a general term used to refer to virus, Trojans, and worms. Malware, depending on their type, may or may not include replicating and non replicating malicious code.
message body	The content of an email message.
Network virus	A virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, a network virus infects the memory of computers, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure.
Notifications	The Security Server can send Administrators a notification whenever significant abnormal events occur on your Clients. For example, you can set up a condition that whenever the Client/Server Security Agent detects 40 virus/malware within one hour, the Security Server will send a notification to the Administrator.
Outbreak Defense	During Outbreak Defense, the Security Server enacts the instructions contained in the Outbreak Prevention Policy. A Trend Micro Outbreak Prevention Policy is a set of recommended default security configurations and settings designed by Trend Micro to give optimal protection to your computers and network during outbreak conditions. The Security Server downloads an Outbreak Prevention Policy from Trend Micro ActiveUpdate Server every 30 minutes or whenever the Security Server starts up. Outbreak Defense enacts preemptive measures such as blocking shared folders, blocking ports, updating components, and running scans.
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.
phishing incident	A Phishing incident starts with an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click a link that will redirect their browsers to a fraudulent Web site. Here the user is asked to update personal information such as passwords, social security numbers, and credit card numbers in an attempt to trick a recipient into providing private information that will be used for identity theft.
Phishing sites	A Web site that lures users into providing personal details, such as credit card information. Links to phishing sites are often sent in bogus email messages disguised as legitimate messages from well-known businesses.
Ping of Death	A Denial of Service attack where a hacker directs an oversized ICMP packet at a target computer. This can cause the computers buffer to overflow, which can freeze or restart the machine.

Term	Description
Plug-ins	Plug-ins are additional modules that enhance protection for your computer or improve the performance. There are many available plug-ins and your administrator needs to enable it before you can use it. Install new or manage installed plug-ins using the Plug-in Manager.
Post Office Protocol 3 (POP3)	POP3 is a standard protocol for storing and transporting email messages from a server to a client email application.
port number	A port number, together with a network address - such as an IP number, allow computers to communicate across a network. Each application program has a unique port number associated with it. Blocking a port on a computer prevents an application associated with that port number from sending or receiving communications to other applications on other computers across a network. Blocking the ports on a computer is an effective way to prevent malicious software from attacking that computer.
privileges (client privileges)	From the Web console, Administrators can set privileges for the Client/Server Security Agents. End users can then set the Client/Server Security Agents to scan their Clients according to the privileges you allowed. Use client privileges to enforce a uniform antivirus policy throughout your organization.
proxy server	A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server.
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
remote	The term "remote" refers to a computer that is connected through a network to another computer, but physically distant from that computer.
rules (content filtering)	Content filtering rules are rules that you set up to filter the content of email messages. You define undesirable content and sources and set the Messaging Security Agent to detect and take action against such content violations.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
Secure Socket Layer (SSL)	SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a public-and-private key encryption system, which also includes the use of a digital certificate.
SSL certificate	A digital certificate that authenticates network entities such as a server or a client.

Term	Description
Web console	The Web console is a centralized Web-based management console. You can use it to configure the settings of Client/Server Security Agents and Messaging Security Agents which are protecting all your remote desktops, servers and Microsoft Exchange servers. The Web console is installed when you install the Trend Micro Security Server and uses Internet technologies such as ActiveX, CGI, HTML, and HTTP.
Security Server	When you first install Worry-Free Business Security Advanced, you install it on a Windows server that becomes the Security Server. The Security Server communicates with the Client/Server Security Agents and the Messaging Security Agents installed on Clients. The Security Server also hosts the Web console, the centralized Web-based management console for the entire Worry-Free Business Security Advanced solution.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses.
Simple Mail Transport Protocol (SMTP)	SMTP is a standard protocol used to transport email messages from server to server, and client to server, over the Internet.
SOCKS	A TCP protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model. The SOCKS 5 protocol, an extension of the SOCKS 4 protocol that offers more choices of authentication
spam	Unsolicited email messages meant to promote a product or service.
Telnet	Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.
Test virus	An inert file that acts like a real virus and is detectable by virus-scanning software. Use test files, such as the EICAR test script, to verify that your antivirus installation is scanning properly.
Transmission Control Protocol (TCP)	A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for 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.

Term	Description
TrendSecure	TrendSecure comprises a set of browser-based plugin tools (TrendProtect and Transaction Protector) that enable users to surf the Web securely. TrendProtect warns users about malicious and Phishing Web sites. Transaction Protector determines the safety of your wireless connection by checking the authenticity of the access point.
Trojan horses	A Trojan horse is a malicious program that is disguised as legitimate software. The term is derived from the classical myth of the Trojan horse.
updates	Updating describe a process of downloading the most updated components such as pattern files and scan engines to your computer.
virus/malware	A virus is a program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes.
vulnerability	A vulnerable computer has weaknesses in its operating system or applications. Many threats exploit these vulnerabilities to cause damage or gain unauthorized control. Therefore, vulnerabilities represent risks not only to each individual computer where they are located, but also to the other computers on your network.
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on.
worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often through email. A worm can also be called a network virus.

Index

A

About
- Client/Server Security Agent 1-8
- Common Firewall Driver 1-12
- keywords 6-21
- Messaging Security Agent 1-9
- Network Virus Pattern File 1-12
- Scan Engine 1-9
- Security Server 1-7
- threats 1-12
- Trend Micro 15-22
- Virus Cleanup Engine 1-11
- Virus Pattern File 1-10
- Vulnerability Pattern File 1-12
- Web console 1-7

ActiveAction 5-7, 6-10, 8-6, 8-10
ActiveUpdate, about 9-3
Add
- tool described 4-6
- using to install Client/Server Security Agent 4-8

Add Group, tool described 4-5
Adding
- Agents 3-1
- alternative update sources 9-10
- Groups 4-6
- Update Agents 9-9

Add-ins 14-13
Administrator's Guide
- how to use P-xv
- information P-xvi

Adware 1-14
Agents
- add 3-1
- configuring 4-6
- Remove 3-21
- Uninstall 3-21

Alerts
- red alert 2-12, 7-12
- yellow alert 2-12, 7-12

Alerts, see Notifications 11-6
Alternative update sources
- adding 9-10
- removing 9-10

Anti-spam
- latest results in Live Status 2-13

Approve URLs 12-7
Approved Programs 5-20
Approved senders
- with End User Quarantine 6-50

Audience P-xiv

B

Backdoors 1-13
Blocked Programs 5-20
Blocking ports, during Outbreak Defense 2-10, 7-3
Blocking shared folders, during Outbreak Defense 7-2
Bots 1-14

C

Capabilities 1-21
Cleanup stage, Outbreak Defense 7-2
Cleanup, during Outbreak Defense 7-3
Client/Server Security Agent
- managing from Security Settings 4-2
- overview 1-8
- using Add to install 4-8
- what's new 1-4

Clients
- configuring 4-6
- move 4-9

Common Firewall Driver 1-12
- overview 1-12

Components
- about 1-17
- conditions for automatic updates 9-2
- downloaded during Outbreak Defense 2-10, 7-3
- rollback 9-14
- synchronize 9-14
- updateable 1-28

Configure, tool described 4-5
Configuring
- Agents, Clients 4-6
- Personal Firewall - Advanced Mode 5-11

Connection Verification 12-12
Contact information 15-19
Content Filtering Rules

changing order 6-35
delete 6-33
enable/disable 6-33
Conventions, document P-xvii
CPU Usage 8-6
Current Status – Cleanup 7-7
Current Status – Prevention 7-3
Current Status – Protection 7-7

D

Damage Cleanup services
how it works 1-11
Decrypting Files 14-8
Default settings
component download source 2-15
notifications 2-6
Outbreak Prevention Policy download schedule 7-12
scheduled updates 9-2
spam threshold 2-13
Defining
Internal Emails 6-51
Deleting
Content Filtering Rules 6-33
logs, automatically 10-11
logs, manually 10-12
one-time reports 10-8
Quarantined Messages 6-46
quarantined messages 6-47
reports 10-9
reports, automatically 10-10
spam messages from Spam folder 6-49
Denied write access, during Outbreak Defense 7-3
Dialers 1-14
Digital Signatures
invalid, troubleshooting 15-17
Disable
alerts 7-14
TrendSecure 5-21
Web Threat Protection 5-15
Document
conventions and terms P-xvii
structure P-xvi
Documentation P-xiv

E

Email Notifications 11-6
Enable
alerts 7-14
TrendSecure 5-21
Web Threat Protection 5-15
Enable/Disable
Content Filtering Rules 6-33
Encrypted and Password protected files 6-7
Encrypted Files
decrypt 14-8
End User Quarantine
disabling 6-48
end user actions 6-50
managing tool 6-49
EUQ 6-51
event thresholds 11-4
Exceptions
Outbreak Defense 7-15
programs 5-20
Exchange Server 2007 15-10
Exchange Servers
real-time scan 6-8
Excluded files (Files over specified scanning restrictions) 6-7
Excluded ports, during Outbreak Defense 7-15
Exclusions
enable/disable 5-6, 8-5
extensions 5-6, 8-5
files 5-6, 8-5
folders 5-6, 8-5
Explicit content
about 1-15
Extensions
exclude from scan 5-6, 8-5
include in scan 5-5, 6-10, 8-5

F

Fake access points
about 1-15
Files
exclude from scan 5-6, 8-5
Firewall
blocks network viruses 1-14
Folders

exclude from scan 5-6, 8-5

G

Generating debugger reports, how to 6-54
Getting Started Guide, how to use P-xiv
Granting Client Privileges 5-25
Groups
adding 4-6
in Security Settings screen 4-4
preserved during upgrade 4-5
replicate settings 4-10

H

Hacking tool 1-14
Help, using icon to access 2-5
Hot Fixes 1-28

I

IM Content Filtering 12-8
Individual settings for Client computers, not supported 4-5
Installing Client/Server Security Agent 4-8
Instant Messaging, See IM Content Filtering
IntelliScan 5-5, 6-10, 8-5, 8-10
Internal Email Definition 6-51
Intrusions
about 1-15
Intuit
FAQ 15-4
protection 5-20

J

Junk E-mail 6-52

K

Key listeners
about 1-15
Keylogger 1-14
Keywords
about 6-21
importing 6-21
operators 6-22
using 6-23
Knowledge Base P-xv, 15-20

L

Language Packs 13-5
License
information in Live Status 2-14
Live Status
viewing 2-7
Logs
automatically deleting 10-11
manually deleting 10-12
Web Threat Protection 12-7

M

Macro viruses 1-13
Maintaining
Spam 6-51
Malicious behavior
about 1-15
Malware 1-13
Managing
Spam 6-51
Mass-mailing attack, defined 1-16
Messaging Security Agent
managing from Security Settings 4-2
overview 1-9
what's new 1-5
Mixed groups 4-5
Move
Clients 4-9
tool described 4-6
MSSQL$SCANMAIL 15-10
Multi-lingual Agents 13-5

N

Network Virus
about 1-14
results in Live Status 2-14
Network Virus Pattern File 1-12
overview 1-12
Notifications
content, modify 11-5
default settings 2-6
delivery method 11-6
setting up 2-6
notifications
events 11-4

thresholds 11-4

O

Official Pattern Release
triggered by red alert 2-12
Online help, how to use P-xiv
Operators 6-22
Outbreak Defense
blocking ports 7-3
blocking shared folders 7-2
cleanup 7-3
cleanup stage 7-2
denying write access 7-3
disabling alerts 7-14
enabling alerts 7-14
excluding ports from blocking 7-15
prevention stage 7-2
protection stage 7-2
scanning 7-3
Security Server actions 7-12
Settings 7-11
stages, table 4-3 7-2
updating components 7-3
vulnerability assessment 7-3
Outbreak Defense Exceptions
add, modify, remove 7-15
enable/disable 7-15
Outbreak Lifecycle, described 7-2
Outbreak Prevention Policy
download frequency 7-15
download source 7-15
downloaded every 30 minutes 7-12

P

Packers, about 1-16
Page Ratings 5-21
Patches 1-28
Phishing incident, defined 1-16
POP3 Mail Scan 5-23
Potential Threat 7-9
Prevention stage, Outbreak Defense 7-2
Privacy Keywords
Programs
exceptions 5-20
Protection 1-17
Intuit programs 5-20
Protection stage, Outbreak Defense 7-2

Q

Quarantined Messages
delete 6-46
resend 6-45

R

Real-time Scan
Exchange Servers 6-8
Red alert 7-12
about 2-12
trigger conditions 2-12
trigger official pattern release 2-12
Refresh 2-5
Regular Expressions 6-24
Remove
Agents 3-21
alternative update sources 9-10
tool described 4-6
Update Agents 9-9
Reorder content filtering rules 6-35
Replacement text or file 6-12, 8-12
Replicate, tool described 4-5
Replicating, Group settings 4-10
Reports
automatically deleting 10-10
debugger 6-53
delete 10-9
edit 10-10
one-time 10-8
Resending
Quarantined Messages 6-45
Reset Counters 4-5–4-6
Rollback
components 9-14
Rootkits 1-13

S

Scan
latest results in Live Status 2-13
Scan Engine
overview 1-9
updates 1-10
ScanMail_Master 15-10

ScanMail_RemoteConfig 15-10
Scanning
  specific files 8-10
  Viruses, Spyware, and Other Malware Threats 8-3
Scanning Extensions 5-5, 6-10, 8-5
Scanning, with IntelliScan 5-5, 6-10, 8-5, 8-10
Scans, during Outbreak Defense 2-10, 7-3
Scheduled Policy Download settings 7-15
Scheduled updates, Security Server
  hourly, by default 9-2
Scheduling
  updates 9-13
Security Groups tree, described 4-2–4-3
Security Server
  action during Outbreak Defense 7-12
  communication with the Security Agents 1-8
  component updates, hourly 9-2
  overview 1-7
  what's new 1-4
Security Settings Toolbar 4-5
Server
  address, checklist A-2
Service Packs 1-28
Simple Mail Transport Protocol (SMTP)
  definition F-7
Smart Protection Network 1-3, 13-5
SNMP Notifications 11-6
SOCKS4
  definition F-7
Software Protection 15-4
Spam 6-51
  about 1-15
  Managing 6-51
Spam Folder
  creating 6-48
  deleting spam messages 6-49
  renaming 6-48
  setting the retention time limit 6-49
Spyware 1-14
SQL Server 15-10
Startup
  automatic update 9-2
Synchronize
  components 9-14

T

Telnet
  definition F-7
Terms, document P-xvii
Test virus
  definition F-7
text/file replacement setting 6-12, 8-12
Threats
  adware 1-14
  backdoors 1-13
  bots 1-14
  dialers 1-14
  explicit content 1-15
  fake access points 1-15
  hacking tools 1-14
  intrusions 1-15
  key listeners 1-15
  keylogger 1-14
  macro viruses 1-13
  malicious behavior 1-15
  malware 1-13
  mass-mailing attacks 1-16
  network virus 1-14
  overview 1-12
  packers 1-16
  phishing 1-16
  rootkits 1-13
  spam 1-15
  spyware 1-14
  Trend Micro protection 1-17
  Trojans 1-13
  worms 1-13
thresholds 11-4
TNEF 14-10
Toolbar 4-5
Transmission Control Protocol (TCP)
  definition F-7
Transport Neutral Encapsulation Format 14-10
Trend Micro ActiveAction C-4
Trend Micro IntelliScan C-4
Trend Micro proxy service 5-24
Trend Micro, about 15-22
TrendLabs
  definition F-7
  updates Virus Cleanup Pattern 1-11

TrendSecure
In Office settings 5-21
Out of Office settings 5-21
Trojans 1-13
definition F-8

U

Unauthorized Changes 5-20
Uninstall
Agents 3-21
Security Server 13-6
Update Agents
adding 9-9
removing 9-9
Update source
ActiveUpdate Server 9-8
Alternate update source 9-9
local copy 9-8
Update Agents 9-9
Updates
automatic 9-2
information in Live Status 2-15
scheduling 9-13
URLs, adding to Approved List 12-7
Using Antivirus to Configure Real-time Scan 5-5
Using Quarantine 5-28

V

Verifying, Agent-Security Server connection 12-12
View approved sender, End User Quarantine command 6-50
Virus
defined 1-12
Virus Cleanup Engine 1-11
overview 1-11
Virus Cleanup Pattern 1-11
Virus Pattern File
overview 1-10
vulnerability assessment, during Outbreak Defense 7-3
Vulnerability Pattern File
overview 1-12

W

Warning
back up before removing third-party antivirus software 15-17
dangers of disabling real-time scanning 6-10
decrypting files 14-9
do not send installation package to wrong Client computer 3-11
never use real virus for testing 3-20
quarantine folder contains email messages that have a high-risk of being infected 6-45
using back up tools 15-11
Web console
major features, overview 2-4
opening 2-2
overview 1-7
Web Reputation Services. See Web Threat Protection
Web Threat Protection 1-26
configure, approved URLs 12-7
In Office settings 5-15
Out of Office settings 5-15
WFBS
documentation P-xiv
overview 1-2
what's included 1-5
WFBS, Capabilities 1-21
What's new 1-2
Wi-Fi Advisor 5-21
Windows Log Notifications 11-6
Worms 1-13

Y

Yellow alert 7-12
about 2-12
trigger conditions 2-13