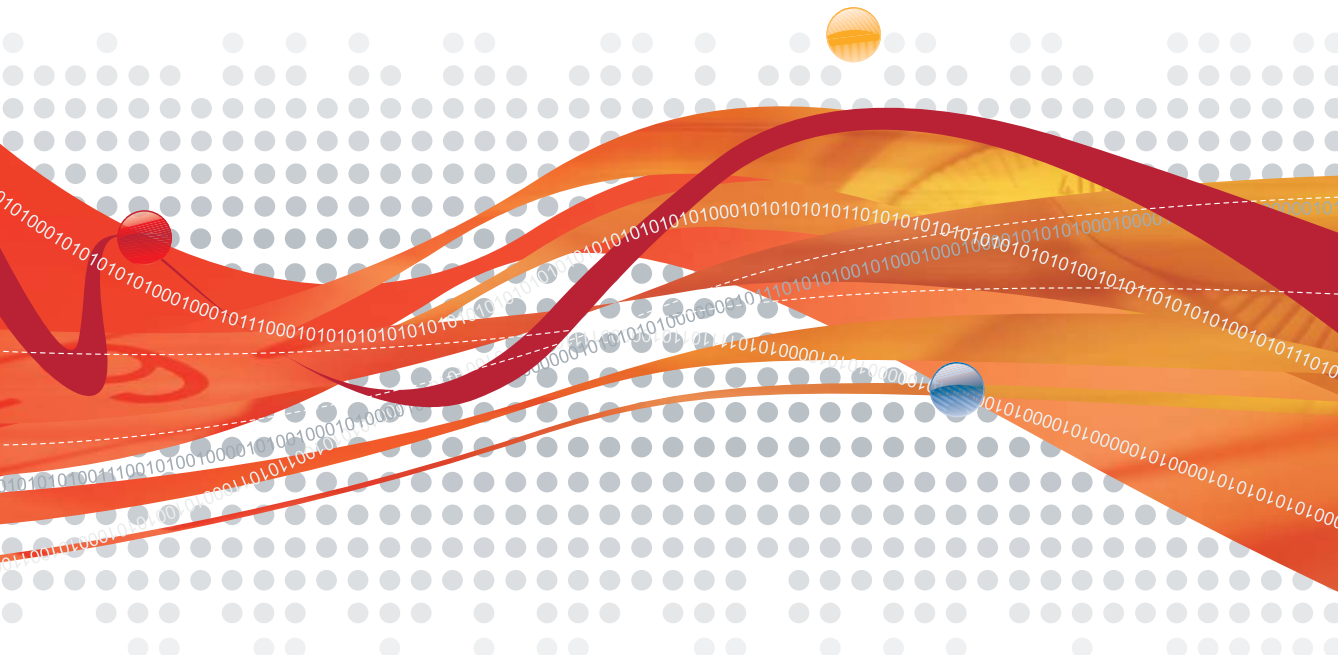
TREND MICRO™

Worry-Free™ Business Security Advanced6

#1 for Small Business Security



Administrator's Guide

Document Part Number: WAEM64047/90311

Release Date: May 2009

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

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

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

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

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

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

Contents

Chapter 4: Managing Groups

Chapter 5: Managing Basic Security Settings

Chapter 6: Managing the Messaging Security Agent

Chapter 7: Using Outbreak Defense

Chapter 8: Managing Scans

Chapter 9: Managing Notifications

Chapter 10: Managing Global Settings

Chapter 11: Managing Updates

Chapter 12: Using Logs and Reports

Chapter 13: Administering WFBS-A

Appendix E: Using Administrative and Client Tools

Appendix F: Troubleshooting and Frequently Asked Questions

Appendix G: Getting Help

Appendix H: Glossary

Index

Chapter 1

Introducing Trend Micro™ Worry-Free™ Business Security Advanced

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

The topics discussed in this chapter include:

Overview of Trend Micro Worry-Free Business Security Advanced

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

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

What's New in This Release?

- **Smart Scan:**

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

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

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

- **URL Web Content Filtering:**

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

- **Smart Protection Network Integration:**

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

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

- **Simpler and Easier Live Status:**

  The Live Status dashboard is now even easier to read.

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

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

- **New graphical interface for Quarantine Tool:**

  Provides easier quarantine management.

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

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

- **Protection from USB autorun threats:**

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

Key Features

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

The Trend Micro Smart Protection Network

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

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products as well as the company's 24/7 threat research centers and technologies. Each new threat identified via a single customer's routine reputation check automatically updates all of the Trend Micro threat databases, blocking any subsequent customer encounters of a given threat. By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in protection of others. Because the threat information gathered is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected.

Web Reputation

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

Email Reputation

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

File Reputation

Trend Micro file reputation technology checks the reputation of each file against an extensive in-the-cloud database before permitting user access. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall client footprint.

Smart Scan

Trend Micro Worry-Free Business Security Advanced uses a new technology called Smart Scan. In the past, WFBS-A clients used Conventional Scan, which involved each client downloading scan-related components to perform scans. With Smart Scan, the client uses the pattern file on the Smart Scan server instead.

The benefits of Smart Scan include:

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

URL Filtering

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

Benefits of Protection

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

TABLE 1-1. Benefits of Protection

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

Components

Antivirus

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

  The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique "signature" or string of tell-tale characters that distinguish it from any other code, the virus experts at Trend Micro capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to patterns in the virus pattern file, searching for a match.
- **Virus pattern:** A file that helps the Security Agents identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.
- **Virus cleanup template:** Used by the Virus Cleanup Engine, this template helps identify Trojan files and Trojan processes, worms, and spyware/grayware so the engine can eliminate them.
- **Virus cleanup engine (32-bit/64-bit):** The engine that Cleanup Services uses to scan for and remove Trojan files and Trojan processes, worms, and spyware/grayware.
- **IntelliTrap exception pattern:** The exception pattern used by IntelliTrap and the scan engines to scan for malicious code in compressed files.
- **IntelliTrap pattern:** The pattern used by IntelliTrap and the scan engines to scan for malicious code in compressed files.
- **Smart Scan Agent Pattern:** The pattern file that the client uses to identify threats. This pattern file is stored on the agent machine.
- **Feedback engine 32-bit** and **64-bit**: The engine for sending feedback to the Trend Micro Smart Protection Network.
- **Smart Scan Pattern:** The pattern file containing data specific to the files on your client's computers.

Anti-spyware

- **Spyware scan engine (32-bit):** A separate scan engine that scans for, detects, and removes spyware/grayware from infected computers and servers running on i386 (32-bit) operating systems.
- **Spyware scan engine (64-bit):** Similar to the spyware/grayware scan engine for 32-bit systems, this scan engine scans for, detects, and removes spyware on x64 (64-bit) operating systems.
- **Spyware pattern:** Contains known spyware signatures and is used by the spyware scan engines (both 32-bit and 64-bit) to detect spyware/grayware on computers and servers for Manual and Scheduled Scans.
- **Spyware active-monitoring pattern:** Similar to the spyware pattern, but is used by the scan engine for anti-spyware scanning.

Anti-spam

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

Outbreak Defense

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

- **Vulnerability pattern:** A file that includes the database for all vulnerabilities.

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

Network Virus

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

Web Reputation

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

TrendProtect

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

Software Protection

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

Behavior Monitoring

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

Transaction Protector

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

Content Filtering

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

Live Status and Notifications

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

Understanding Threats

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

Virus/Malware

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

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

- **Malware:** Malware is software designed to infiltrate or damage a computer system without the owner's informed consent.
- **Trojans:** A Trojan is a malicious program that masquerades as a harmless application. Unlike virus/malware, Trojans do not replicate but can be just as destructive. An application that claims to rid your computer of virus/malware when it actually introduces virus/malware into your computer is an example of a Trojan.
- **Worms:** A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments. Unlike virus/malware, worms do not need to attach themselves to host programs.
- **Backdoors:** A backdoor is a method of bypassing normal authentication, securing remote access to a computer, and/or obtaining access to information, while attempting to remain undetected.
- **Rootkit:** A rootkit is a set of programs designed to corrupt the legitimate control of an operating system by its users. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security.

- **Macro Viruses:** Macro viruses are application-specific. The viruses reside within files for applications such as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications such as .doc, .xls, and .ppt. Macro viruses travel amongst data files in the application and can eventually infect hundreds of files if undeterred.

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

Spyware/Grayware

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

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

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

Network Viruses

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

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

Spam

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

Intrusions

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

Malicious Behavior

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

Fake Access Points

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

Explicit/Restricted Content in IM Applications

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

Online Keystroke Listeners

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

Product Component Terminology

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

TABLE 1-2. Product Component Terminology

ITEM	DESCRIPTION
Security Server	The Security Server hosts the Web console, the centralized Web-based management console for the entire WFBS-A solution.
Scan Server	A Scan Server helps scan clients that are configured for Smart Scan. By default, a Scan Server is installed on the Security Server.
Agent/CSA/MSA	The Client/Server Security Agent or Messaging Security Agent. Agents protect the client it is installed on.
Client	Clients are Microsoft Exchange servers, desktops, portable computers, and servers where a Messaging Security Agent or a Client/Server Security Agent is installed.
Web console	The Web console is a centralized, Web-based, management console that manages all the Agents. The Web console resides on the Security Server.

Chapter 2

Getting Started

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

The topics discussed in this chapter include:

Accessing the Web Console

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

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.

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

To open the Web console:

1. Select one of the following options to open the Web console:
   - Click the **Worry-Free Business Security** shortcut on the Desktop.
   - From the Windows™ Start menu, click **Trend Micro Worry-Free Business Security > Worry-Free Business Security**.

- You can also open the Web console from any computer on the network. Open a Web browser and type the following in the address bar:
  `https://{Security_Server_Name}:{port number}/SMB`

  For example:

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

  `https://192.168.0.10:4343/SMB`

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

  `http://192.168.0.10:8059/SMB`

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

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

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

FIGURE 2-1. Logon screen of WFBS-A

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

Web Console Icons

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

TABLE 2-2. Web Console Icons

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

Live Status

Use the Live Status screen to manage WFBS-A.

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**.

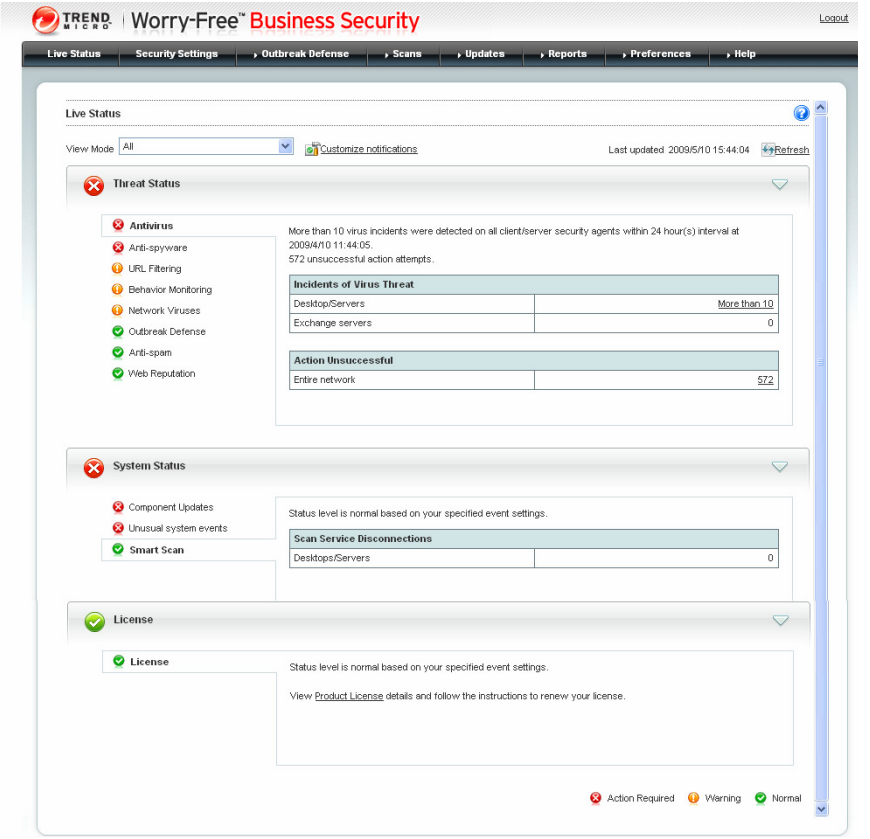


FIGURE 2-2. Live Status screen

Understanding Icons

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

TABLE 2-3. Live Status Icons

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

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

Threat Status

The Threat Status screen displays information about the following:

- **Antivirus:** virus detections. Starting from the 5th incident, the status icon changes to display the Warning. If you must take action:
  - The Client/Server Security Agent did not successfully perform the action it was set up to perform. Click the numbered link to view detailed information about computers on which the Client/Server Security Agent was unable to perform and take an action.
  - Real-time scanning is disabled on Client/Server Security Agents. Click **Enable Now** to start Real-time scanning again.
  - The real-time scanning is disabled on the Messaging Security Agent.
- **Anti-spyware:** The Anti-spyware section displays the latest spyware scan results and spyware log entries. The Number of Incidents column of the Spyware Threat Incidents table displays the results of the latest spyware scan.
  - To find more information about specific clients, click the number link under the **Incidents Detected** column of the Spyware Threat Incidents table. From there, you can find information about the specific spyware threats that are affecting your clients.
- **URL Filtering:** restricted Web sites as determined by the administrator. Starting from the 300th incident, the status icon changes to display the warning.
- **Behavior Monitoring:** violations of the behavior monitoring policies.
- **Network Viruses:** network virus detections determined by the firewall settings.
- **Outbreak Defense:** a possible virus outbreak on your network.
- **Anti-spam:** spam detections. Click the **High**, **Medium**, or **Low** link to be redirected to the configuration screen for the selected Microsoft Exchange server where you can set the threshold level from the Anti-spam screen. Click **Disabled** to be redirected to the appropriate screen. This information is updated on an hourly basis.
- **Web Reputation:** potentially dangerous Web sites as determined by Trend Micro. Starting from the 200th incident, the status icon changes to display the warning.

System Status

View information regarding the updated components and the free space on computers where agents are installed.

- **Component Updates:** the status of component updates for the Security Server or the deployment of updated components to agents.
- **Unusual system events:** disk space information about clients that are functioning as servers (running server operating systems).
- **Smart Scan:** the clients that cannot connect to their assigned scan server.

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

License Status

View information regarding the license status.

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

Live Status Update Intervals

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

TABLE 2-4. Live Status Update Intervals

Item	Update Interval (minutes)	Agent Sends Logs to Server After... (minutes)
Outbreak Defense	3	N/A
Antivirus	1	CSA: Immediate MSA: 5
Anti-spyware	3	1
Anti-spam	3	60

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

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

Viewing Security Settings

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

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

Global Navigation Menu

These menu items remain available regardless of the options selected in the Security Settings screen are constant for all other screens.

Configuration Area

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

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

Toolbar:

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

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

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

- **Replicate Settings:** The Replicate Settings tool is only available when one of the items in the Security Groups Tree is selected and there is at least one other item of the same type in the Security Groups Tree.
- **Import/Export Settings:** Save your configuration settings or import settings that you have already saved.
- **Add Group:** The Add Group tool allows you to add new desktop or server groups.
- **Add:** The Add tool allows you to add computers to specific groups by deploying Client/Server Security Agents to computers you specify.
- **Remove:** The Remove tool will remove the agent from the computers that you specify.
- **Move:** The Move tool allows you to move selected computer or servers from one security server to another.

- **Reset Counters:** The Reset Counters tool works on all computers within a group. When clicked, the value in the Viruses Detected and Spyware Detected columns of the Security Agent information table will be reset to zero.
- **Security Groups Tree:** Select a group from the Security Groups Tree to display a list of computers in that group to the right.
- **Security Agent information table:** When you select a client and click a tool from the toolbar, the Web console displays a new configurations area.

Chapter 3

Installing Agents

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

The topics discussed in this chapter include:

Agent Installation Overview

WFBS-A 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 3-4)
- **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 3-6)
- **Client Packager:** Deploy the Client/Server Security Agent setup or update files to clients through email (see *Installing with Client Packager* on page 3-8)
- **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 3-11)
- **Vulnerability Scanner (TMVS):** Install the Client/Server Security Agent on all Windows 2000/Server 2003 clients with the Trend Micro Vulnerability Scanner (*Installing with Vulnerability Scanner* on page 3-14)

TABLE 3-1. 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.

Agent Installation/Upgrade/Migration Overview

This section provides information on the following:

- Performing a fresh Client/Server Security Agent install with your chosen installation method (see *Agent Installation Overview* 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 WFBS-A (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.

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, 6.0, or 7.0 or Apache™ 2.0.63, 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 *Verifying Client Installation with Vulnerability Scanner* on page 3-18 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
   ```

   For example:

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

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

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

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

   - For Conventional Scan: 
   - For Smart Scan: 

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 WFBS-A, 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 Scripts

If you already have an existing login script for Windows 2000/Server 2003/Server 2008, Login Script Setup will append a command that executes `autopcc.exe`; otherwise, it creates a batch file called `ofcscan.bat` (contains the command to run `autopcc.exe`).

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

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

where:

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

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

The 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. agents installed using Client Packager report to the server where Client Packager created the setup package. This tool is especially useful when deploying the agent or update files to clients in low-bandwidth remote offices.

Client Packager Installation Considerations

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

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

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 **Scan Mode**.
   - **Conventional Scan:** a local scan engine on the client scans the client computer.
   - **Smart Scan:** a Scan Server helps scan the client. A Scan Server is automatically installed with the security server. You can choose the scan method on the Security Settings screen. Scan modes use different pattern files. Conventional Scan uses the traditional virus pattern file.

6. 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.
7. Select from among the following installation options under **Options**:
   - **Silent Mode:** Creates a package that installs on the client in the background, unnoticeable to the user. The installation status window will not appear.
   - **MSI Package:** Creates a package that conforms to the Microsoft Windows Installer Package Format.

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

   - **Disable Prescan (only for fresh-install):** Disables the normal file scanning that WFBS-A performs before starting setup.
8. 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.
9. Ensure that the location of the `ofcscan.ini` file is correct next to **Source file**. To modify the path, click ... to browse for the `ofcscan.ini` file. By default, this file is located in the `\PCCSRV` folder of the Trend Micro Security Server.

10. In **Output file**, click ... to specify the file name (for example, `ClientSetup.exe`) and the location to create the package.
11. Click **Create** to build the package. When Client Packager finishes creating the package, the message **Package created successfully** appears. To verify successful package creation, check the output directory you specified.
12. Send the package to your users through email, or copy it to a CD or similar media and distribute among your users.

WARNING! **You can only send the package to 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. For instructions on creating an MSI file, see *Installing with Client Packager* on page 3-8.

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 WFBS-A 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 *Verifying Client Installation with Vulnerability Scanner* on page 3-18.

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: **{server location}** > **PCCSRV** > **Admin** > **Utility** > **TMVS**. Double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears.
2. Click **Settings**. The **Settings** screen appears.

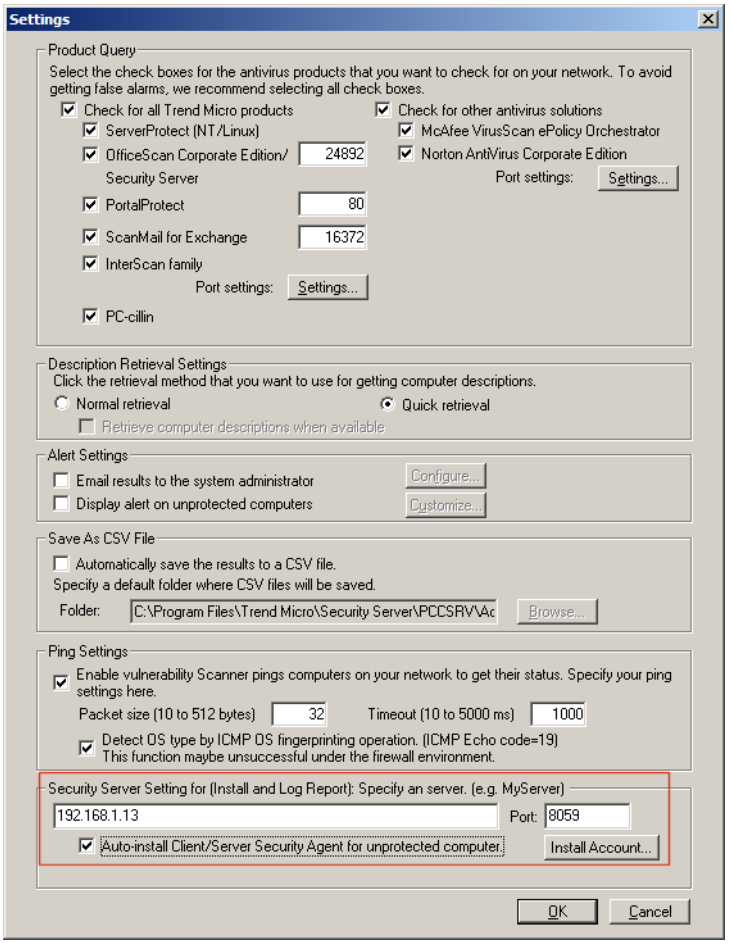


FIGURE 3-1. TMVS Settings screen

3. Under **Trend Micro Security Server Setting (for Install and Log Report)**, type the Trend Micro Security Server name or IP address and port number.
4. Select the **Auto-install** 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 with Email Notification

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

To notify the location of the package from the console:

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

Installing MSA from the Web Console

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. For the **Spam Management Type**, **End User Quarantine** will be used.
8. Under **Directories**, change or accept the default target and shared directories for the MSA installation. The default target and shared directories are `C:\Program Files\Trend Micro\Messaging Security Agent` and `C$`, respectively.
9. Click **Next**. The Microsoft Exchange Server Settings screen appears.
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 WFBS-A program shortcuts on the Windows **Start** menu of the client running the agent.
- Check if WFBS-A is in the **Add/Remove Programs** list of the client's Control Panel.
- Use Vulnerability Scanner (see *Verifying Client Installation with Vulnerability Scanner* on page 3-18).
- Use the Client Mover tool.

Verifying Client Installation with Vulnerability Scanner

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

Testing the Client Installation with the EICAR Test Script

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

Obtaining the EICAR Test File:

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

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

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

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

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

Removing Agents

There are two ways to remove agents:

- Running the agent uninstallation program
- Using the Web console

WARNING! Removing agents makes clients vulnerable to threats.

Removing the Agent Using the Agent Uninstallation Program

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

To run the Agent uninstallation program:

1. On the Windows **Start** menu, click **Settings > Control Panel > Add or Remove Programs**.
2. Select **Trend Micro** 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**.

Removing the Agent Using the Web Console

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

To remotely remove an Agent using the Web console:

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

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

Removing the Agent from Exchange Servers

To remove Messaging Security Agent using the Web console:

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

Running the Messaging Security Agent Uninstallation Program

To remove the Messaging Security Agent:

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

Chapter 4

Managing Groups

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

The topics discussed in this chapter include:

Overview of Groups

In WFBS-A, 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. Microsoft Exchange servers cannot be grouped together. To configure Microsoft Exchange servers, refer to *Configurable Options for the Messaging Security Agent* on page 6-6.

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

Viewing Clients in a Group

Navigation Path: Security Settings > Select 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.

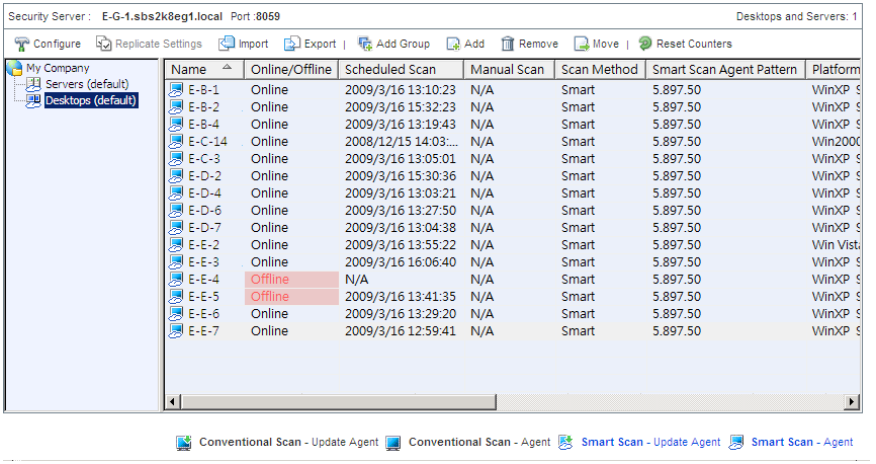


FIGURE 4-1. Security Settings screen showing clients in a group

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. Use the information on this screen to:

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

From here you can:

- **Configure groups:** Refer to *Adding Groups* on page 4-5.
- **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 4-5.
- **Remove groups:** Refer to *Removing Computers and Groups from the Web Console* on page 4-6.
- **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.

Adding Groups

Navigation Path: Security Settings > Add Group

Create groups to collectively manage multiple clients.

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

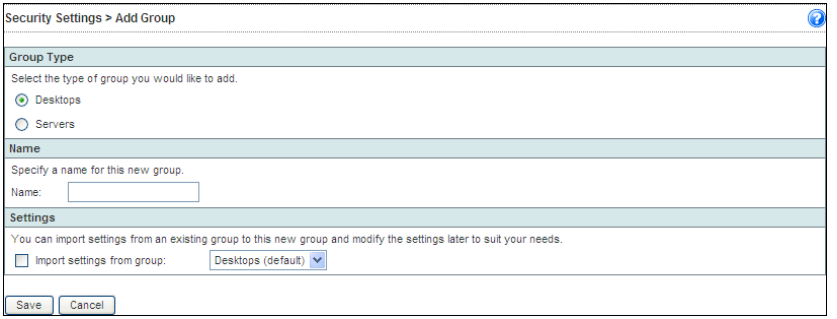


FIGURE 4-2. Add Group screen

To add a group:

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

Removing Computers and Groups from the Web Console

Navigation Path: Security Settings > Select a Group

You can use Remove to accomplish two goals:

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

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

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

To remove a Client or group:

1. Click the group or computer that you want to remove.
2. Click **Remove** from the toolbar.
   - Select **Remove the selected inactive agent(s)** to remove the client icon from the Web console.
   - Select **Uninstall the selected agent(s)** to remove the Client/Server Security Agent from the selected computers and remove the computer icons from the Web console.
3. Click **Apply**.

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

Adding Clients to Groups

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

Tip: In organizations where IT policies are strictly enforced, Remote Install and Login Script Setup are recommended.

- **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
- **Login Script Setup:** Automate the installation of the Client/Server Security Agent to unprotected computers when they log on to the domain
- **Client Packager:** Deploy the Client/Server Security Agent setup or update files to Clients through email
- **Installing with Email Notification:** Send an email message with a link to the installer.
- **Remote Install:** Install the Agent on all Windows Vista/2000/XP/Server 2003/Server 2008 Clients from the Web console
- **Vulnerability Scanner (TMVS):** Install the Client/Server Security Agent on all Windows 2000/Server 2003 clients with the Trend Micro Vulnerability Scanner

When you add a desktop or server, the Security Server deploys an agent to the computer and adds the icon for that client to the Security Settings screen. Once the agent is installed on your client, it will start to report security information to the Security Server.

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

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 3-11 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 3-6 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.

Moving Clients

Navigation Path: Security Settings > Select a Group

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

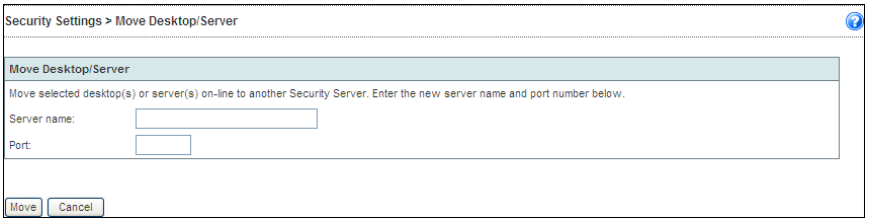


FIGURE 4-3. Move Desktop/Server screen

To move a Client from one Group to another:

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

To move a Client from one Security Server to another:

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

Replicating Group Settings

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

Navigation Path: Security Settings > Select a Group

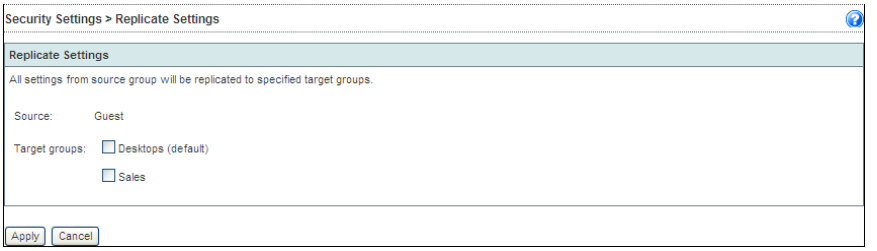


FIGURE 4-4. Replicate Settings screen

To replicate settings from one group to another:

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

Importing and Exporting Settings

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

- **In Security Settings:**

  Antivirus/Anti-Spyware, Firewall, Web Reputation, URL Filtering, Behavior Monitoring, Trend Secure Toolbar, Mail Scan, Client Privilege, Quarantine

- **In Scans:**

  Manual Scan, Scheduled Scan

Note: You can import/export settings between desktops and servers. Settings are not dependent on group type.

To import settings:

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

To export settings:

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

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

Chapter 5

Managing Basic Security Settings

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

The topics discussed in this chapter include:

Options for Desktop and Server Groups

In WFBS-A, Groups are a collection of clients that share the same configuration and run the same tasks. By grouping clients, simultaneously configure and manage, multiple clients. For more information, refer to *Overview of Groups* on page 4-2.

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

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

Option	Description	Default
Scan Method	Switch between Smart Scan and Conventional Scan	Conventional Scan (for upgrade) Smart Scan (for new installation)
Antivirus/Anti-spyware	Configure Real-time Scan, antivirus, and anti-spyware options	Enabled (Real-time Scan)
Firewall	Configure Firewall options	Disabled
Web Reputation	Configure In Office and Out of Office Web Reputation options	In Office: Enabled, Low Out of Office: Enabled, Medium
Behavior Monitoring	Configure Behavior Monitoring options	Enabled
URL Filtering	URL filtering blocks Web sites that violate configured policies.	Enabled
TrendSecure	Configure In Office and Out of Office options for Transaction Protector and TrendProtect	In Office: Disabled Out of Office: Enabled
POP3 Mail Scan	Configure the scanning of POP3 email messages	Disabled
Client Privileges	Configure access to settings from the client console	N/A

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

Option	Description	Default
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.

About Scan Types

Virus scanning is a central part of the Worry-Free Business Security strategy. During a scan, the Trend Micro scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique signature or string of tell-tale characters that distinguish it from any other code, the virus experts at TrendLabs capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match.

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

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

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

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

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

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

  To configure a Manual Scan, click **Scans > Manual Scan**. Refer to *Configuring Manual and Scheduled Scan Options* and *Configuring Scan Options for Microsoft Exchange Servers* 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 your clients and improve the efficiency of threat management.

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

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

Configuring Real-time Scan

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

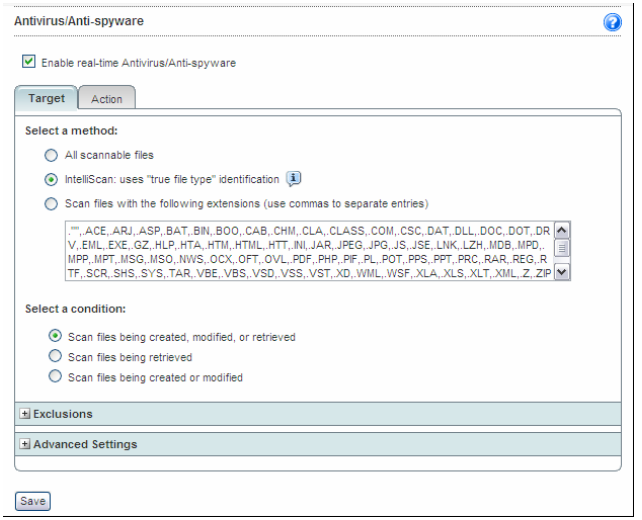


FIGURE 5-1. Security Settings > Antivirus/Anti-spyware screen

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:** WFBS-A 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 8-7 for more information.

2. From the **Action** tab on the **Antivirus/Anti-spyware** screen, specify how WFBS-A 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, WFBS-A could delete related registry entries, files, cookies, and shortcuts. Processes related to the spyware/grayware could also be terminated.
     - **Deny Access**

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

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

3. Click **Save.**

   Additionally, configure who receives notifications when an event occurs. Refer to *Configuring Events for Notifications* on page 9-3.

Managing the Firewall

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

WFBS-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.

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 5-2. Default Firewall Settings

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

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

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

Location	Firewall Settings
In Office	Off
Out of Office	Off

Traffic Filtering

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

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

Scanning for Network Viruses

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

Stateful Inspection

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

Intrusion Detection System

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

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

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

Stateful Inspection

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

Configuring the Firewall

Note: Configure the Firewall for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. Refer to *Location Awareness* on page 10-6.

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

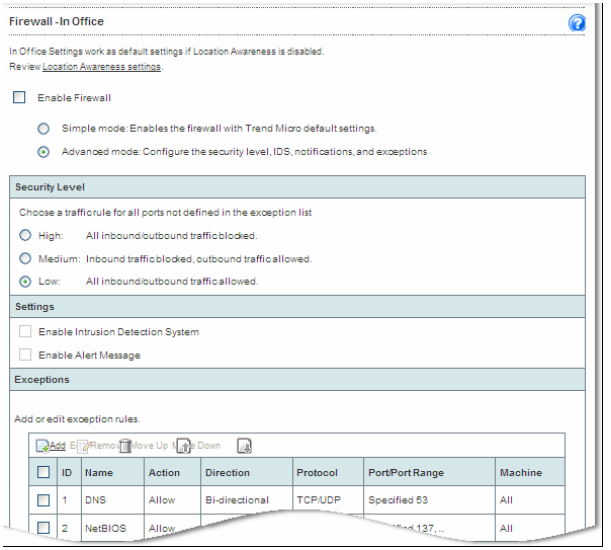


FIGURE 5-2. Firewall - In Office screen

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 5-9.
     - **Advanced Mode:** Enables firewall with custom settings. Refer to *Advanced Firewall Options* on page 5-13 for configuration options.
2. Click **Save.** The changes take effect immediately.

Advanced Firewall Options

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

To configure advanced firewall options:

1. From the **Firewall** screen, select **Advanced Mode**.
2. Update the following options as required:
   - **Security Level:** The security level controls the traffic rules to be enforced for ports not in the exception list.
     - **High:** Blocks inbound and outbound traffic.
     - **Medium:** Blocks inbound traffic and allows outbound.
     - **Low:** Allows inbound and outbound traffic.
   - Settings
     - **Enable Intrusion Detection System:** Intrusion Detection System identifies patterns in network packets that may indicate an attack. Refer to *Intrusion Detection System* on page 5-10 for more information.
     - **Enable Alert Messages:** When WFBS-A detects a violation, the client is notified.
   - **Exceptions:** Ports in the exception list will not be blocked. Refer to *Working with Firewall Exceptions* on page 5-15 for more information.
3. Click **Save**.

Disabling the Firewall

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

To disable the Firewall:

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

Note: To completely disable the Firewall, repeat the above process for both connection types (In Office and Out of Office).

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 5-15 for more information.
4. Click **Save.**

Removing Exceptions

To remove an exception:

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

Using Web Reputation

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

If Web Reputation blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list. For information on adding a URL to the Approved URL list, refer to *Approved URLs* on page 10-8 for more details.

Configuring Web Reputation

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

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

Note: Configure the Web Reputation settings for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. Refer to *Location Awareness* on page 10-6.

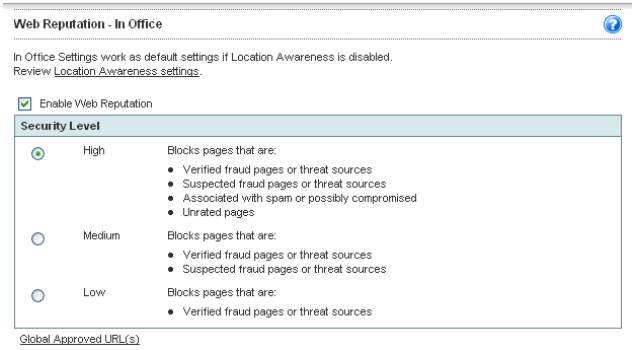


FIGURE 5-3. Security Settings > Web Reputation screen

To edit Web Reputation settings:

1. From the **Web Reputation** screen, update the following as required:
   - **Enable Web Reputation**
   - **Security Level**
     - **High:** Blocks pages that are verified fraud pages or threat sources, suspected fraud pages or threat sources, associated with spam or possibly compromised, unrated pages
     - **Medium:** Blocks pages that are verified fraud pages or threat sources, suspected fraud pages or threat sources
     - **Low:** Blocks pages that are verified fraud pages or threat sources

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

Configuring URL Filtering

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

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

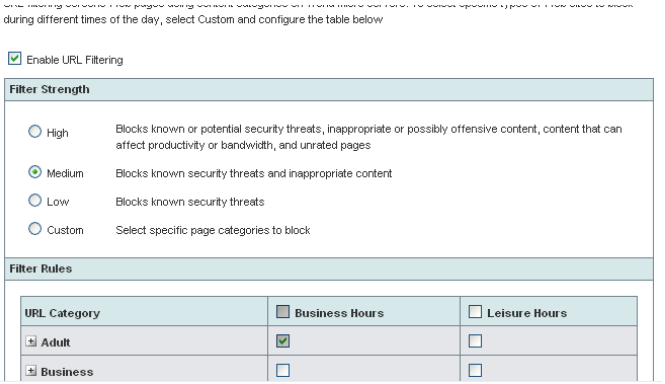


FIGURE 5-4. Security Settings > URL Filtering screen

To configure URL Filtering:

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

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

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

Using Behavior Monitoring

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

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

TABLE 5-3. Possible Changes Monitored

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

TABLE 5-3. Possible Changes Monitored (Continued)

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

TABLE 5-3. Possible Changes Monitored (Continued)

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

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

Configuring Behavior Monitoring

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

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

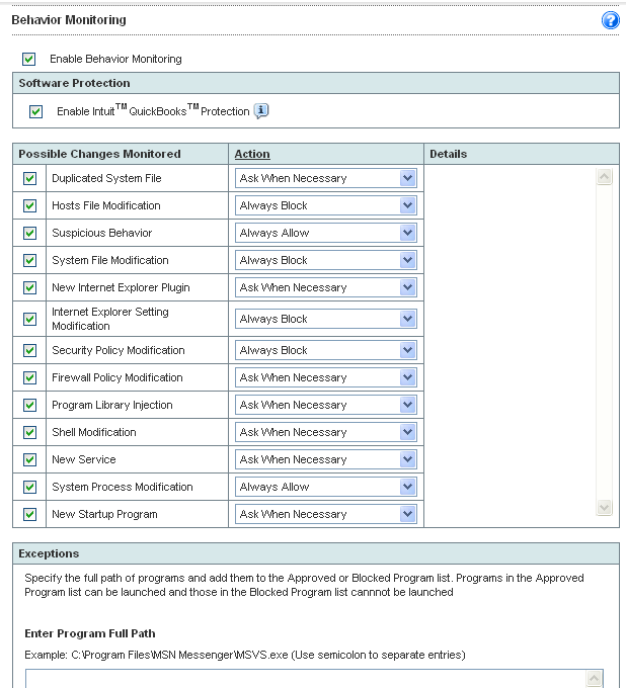


FIGURE 5-5. Behavior Monitoring screen

To edit Behavior Monitoring settings:

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

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

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

     The following products are supported:

     QuickBooks Simple Start

     QuickBooks Pro

     QuickBooks Premier

     QuickBooks Online
   - **Prevent applications in USB plug-in devices from automatically opening:** Select this option to stop programs on USB devices from running automatically on clients.
   - **Possible Changes Monitored:** Select **Always Allow**, **Ask When Necessary**, or **Always Block** for each monitored change. Refer to Table 5-3 on page 5-19 for information on the different changes.
   - **Exceptions:** Exceptions include an **Approved Program List** and a **Blocked Program List**: Programs in the **Approved Programs List** can be started even if it violates a monitored change, while programs in the **Blocked Program List** can never be started.
     - **Full Path of Program:** Type the full 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 5-4* on page 5-24 for the list of supported variables.
     - **Approved Programs List:** Programs (maximum of 100) in this list can be started. Click the corresponding  icon to delete an entry.

- **Blocked Programs List:** Programs (maximum of 100) in this list can never be started. Click the corresponding  icon to delete an entry.

2. Click **Save**.

Environment Variables

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

TABLE 5-4. Supported Variables

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

TrendSecure

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

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

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

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

Note: Configure the TrendSecure settings for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. Refer to *Location Awareness* on page 10-6.

Configuring TrendSecure

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

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

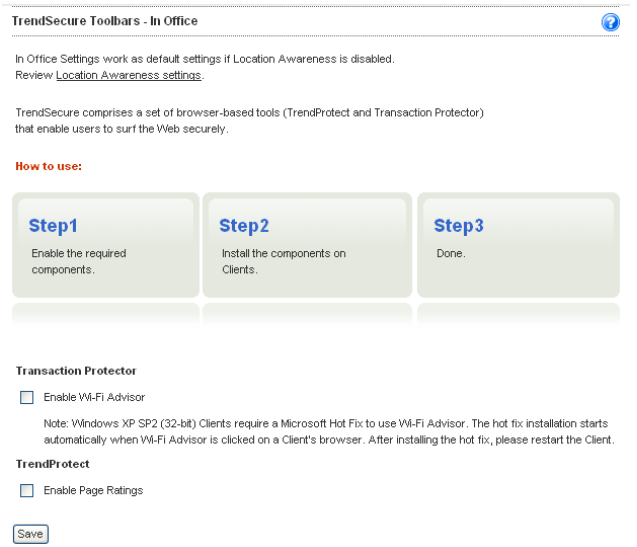


FIGURE 5-6. TrendSecure Toolbars - In Office screen

To edit the availability of TrendSecure tools:

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

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

Managing POP3 Mail Scan

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

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

POP3 Mail Scan Requirements

POP3 Mail Scan supports the following mail clients:

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

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

Anti-Spam Toolbar Requirements

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

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

The Anti-Spam toolbar supports the following operating systems:

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

Configuring Mail Scan

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

To edit the availability of Mail Scan:

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

Client Privileges

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

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

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

Configuring Client Privileges

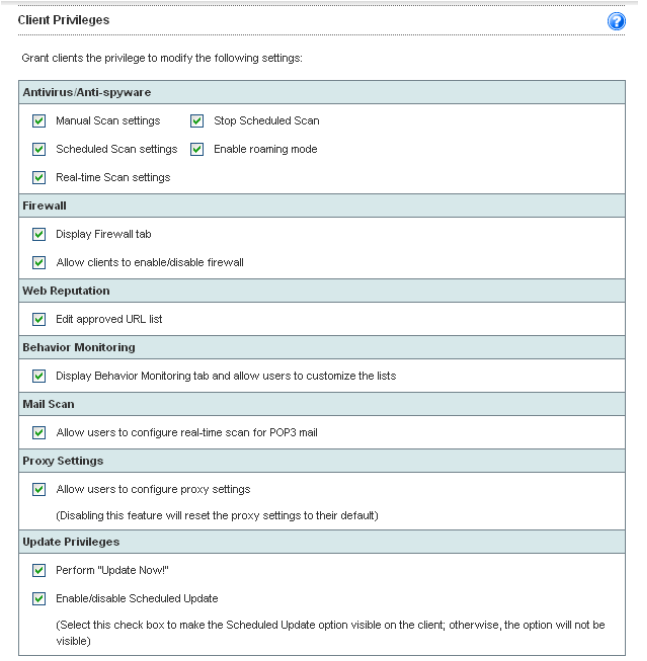


FIGURE 5-7. Client Privileges screen

To grant privileges to Clients:

1. From the **Client Privileges** screen, update the following as required:
   - **Antivirus/Anti-spyware**
     - **Manual Scan settings**
     - **Scheduled Scan settings**
     - **Real-time Scan settings**
     - **Stop Scheduled Scan**
     - **Enable roaming mode**
   - **Firewall**
     - **Display Firewall tab**
     - **Allow clients to enable/disable firewall**

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

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

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

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

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

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

---

2. Click **Save**.

Managing the Quarantine

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

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

The default folder on the server is:

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

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

Configuring the Quarantine Directory

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

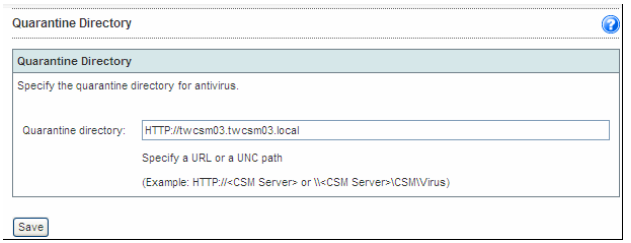


FIGURE 5-8. Quarantine Directory screen

To set the Quarantine directory:

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

Chapter 6

Managing the Messaging Security Agent

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

Messaging Security Agents (MSAs) 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.

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

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

How the Messaging Security Agent Scans Email Messages

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

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

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. During a manual or Scheduled Scan, the Messaging Security Agent updates the Information Store and replaces the file with the cleaned one.
Replace with text/file	The Messaging Security Agent deletes the infected content and replaces it with text or a file. The email message is delivered to the intended recipient, but the text replacement informs them that the original content was infected and was replaced.
Quarantine entire message	Moves the email message to a restricted access folder, removing it as a security risk to the Microsoft Exchange environment. The original recipient will not receive the message. This option is not available in Manual and Scheduled Scanning. See *Configuring Quarantine Directories* on page 6-46 for more information about the quarantine folder.

TABLE 6-1. Messaging Security Agent Customized Actions (Continued)

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

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 the Messaging Security Agent

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

- **Antivirus:** Configure Real-time Scan options for the Messaging Security Agent.
- **Anti-spam (Content Scanning):** Set spam detection level, configure Approved/Blocked Senders list, and set actions for spam.
- **Anti-Spam (Email Reputation):** Configure Email Reputation to block messages from known or suspected sources of spam. Additionally, create exclusions to allow or block message from other senders
- **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 the table 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 the Outlook Junk Email or 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
Attachment blocking		
Action	Replace attachment with text/file	Replace attachment with text/file

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

Scan option	Real-time Scan	Manual and Scheduled Scan
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

WFBS-A 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, WFBS-A takes actions against threats according to the actions set by the Administrator.
- **Scheduled Scan:** A Scheduled Scan is similar to Manual Scan but scans all files and email messages at the configured time and frequency. Use Scheduled Scans to automate routine scans on clients and improve threat management efficiency.

Configuring Real-time Scan for Messaging Security Agents

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Antivirus

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 6-7 for the default settings.

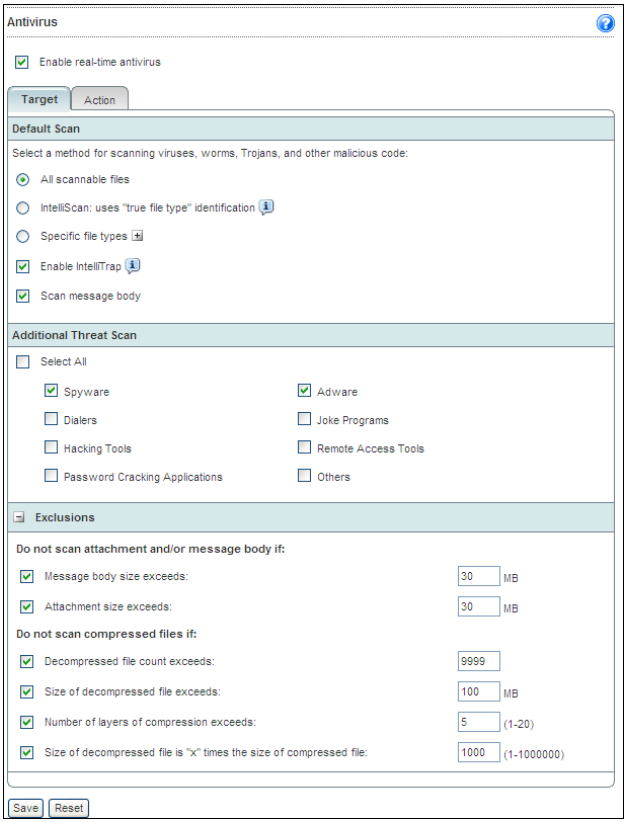


FIGURE 6-1. Security Settings > Antivirus screen

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

Note: The following file types are always .com, ASCII, TEXT, HTML, and Active Server pages.

  - **Enable IntelliTrap:** IntelliTrap detects malicious code such as bots in compressed files. 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 WFBS-A should scan. Refer to *Understanding Threats* on page 1-12 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 6-4 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 6-4 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 6-4 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:** WFBS-A will send notification messages to the selected people. Administrators can also disable sending notifications to spoofing senders.
- **Macros:** A type of virus encoded in an application macro and often included in a document. Select **Enable advanced macro scan** and configure the following:
  - **Heuristic level:** Heuristic scanning is an evaluative method of detecting viruses. This method excels at detecting undiscovered viruses and threats that do not have a known virus signature.
  - **Delete all macros detected by advanced macro scan:** Refer to *Advanced Macro Scanning* on page 6-6 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, WFBS-A will replace the threat with this text string and file.

3. Click **Save.**

   Additionally, configure who receives notifications when an event occurs. Refer to *Configuring Events for Notifications* on page 9-3.

Anti-Spam

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

Email Reputation

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

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

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

Configuring Email Reputation

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Anti-Spam > Email Reputation

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

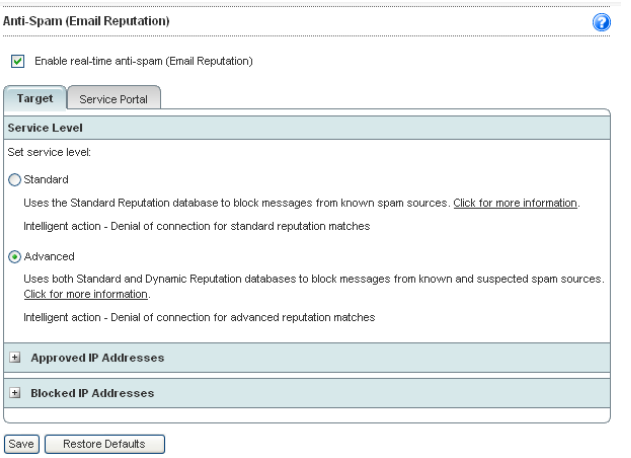


FIGURE 6-2. Email Reputation screen

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 6-13 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

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 marks (!!!!) in their email messages. When the Messaging Security Agent detects a message that uses exclamation marks in this way, it increases the spam score for that email message.

Select one of these options for your spam detection:

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

The Messaging Security Agent 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

TABLE 6-3. Email Address Matches for Wildcards (Continued)

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

Configuring Content Scanning

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Anti-Spam > Content Scanning

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

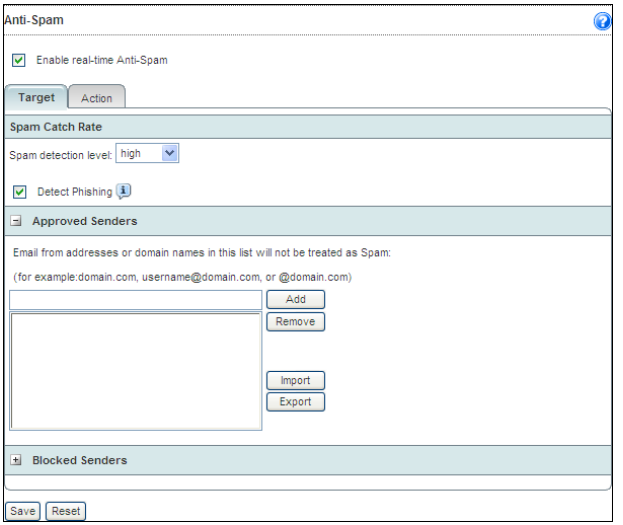


FIGURE 6-3. Content Scanning screen

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 6-15 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 6-16 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 6-17 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 6-17 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.

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.

Keywords

In WFBS-A, keywords include the following and are used to filter messages:

- Words (guns, bombs, and so on)
- Numbers (1,2,3, and so on)

- Special characters (&,#,+, and so on)
- Short phrases (blue fish, red phone, big house, and so on)
- Words or phrases connected by logical operators (`apples .AND. oranges`)
- Words or phrases that use *regular expressions* (`.REG. a.*e` matches "ace", "ate", and "advance", but not "all", "any", or "antivirus")

Importing Keywords

WFBS-A 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"

TABLE 6-4. Using Operators (Continued)

OPERATOR	HOW IT WORKS	EXAMPLE
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 (Continued)

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 6-29 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 6-29.
- 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."

TABLE 6-5. How to Use Keywords (Continued)

SITUATION	EXAMPLE	MATCH/NON-MATCH
Two words separated by a comma	guns, bombs	Matches: "Click here to buy guns, bombs, and other weapons." Does not match: "Click here to buy used guns, new bombs, and other weapons."

TABLE 6-5. How to Use Keywords (Continued)

SITUATION	EXAMPLE	MATCH/NON-MATCH
Multiple words on multiple lines	guns bombs weapons and ammo	When you choose **Any specified keywords** Matches: "Guns for sale" Also matches: "Buy guns, bombs, and other weapons" When you choose **All specified keywords** Matches: "Buy guns bombs weapons and ammo" Does not match: "Buy guns bombs weapons ammunition." Also does not match: "Buy guns, bombs, weapons, and ammo"
Many keywords on same line	guns bombs weapons ammo	Matches: "Buy guns bombs weapons ammo" Does not match: "Buy ammunition for your guns and weapons and new bombs"

Regular Expressions

Regular expressions are used to perform string matching. See the following tables for some common examples of regular expressions. To specify a *regular expression*, add a ".REG." operator before that pattern.

There are a number of 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 recommends is to start with simple regular expressions that do not use complex syntax. When introducing new rules, use the archive action and observe how 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

TABLE 6-6. Counting and Grouping (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
?	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."
[ ]	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.

TABLE 6-6. Counting and Grouping (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
{ }	Curly brace characters set a specific number of occurrences of the preceding element. A single value inside the braces means that only that many occurrences will match. A pair of numbers separated by a comma represents a set of valid counts of the preceding character. A single digit followed by a comma means there is no upper bound.	da{3} matches daaa--d followed by 3 and only 3 occurrences of “a”. da{2,4} matches daa, daaa, daaaa, and daaaa (but not daaaaa)--d followed by 2, 3, or 4 occurrences of “a”. da{4,} matches daaaa, daaaaa, daaaaaa, etc.--d followed by 4 or more occurrences of “a”.

TABLE 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.
\w	Any “word” character--that is, any alphanumeric character; functionally equivalent to [_A-Za-z0-9] or [_[:alnum:]]	**\w** matches a, ab, a1, but not !&--one or more upper- or lower-case letters or digits, but not punctuation or other special characters.
\W	Any non-alphanumeric character; functionally equivalent to [^_A-Za-z0-9] or [^_[:alnum:]]	**\W** matches *, &, but not ace or a1--one or more of any character but upper- or lower-case letters and digits.

TABLE 6-7. Character Classes (shorthand) (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
\s	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [[: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 (Continued)

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, !@#.

TABLE 6-8. Character Classes (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
[: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.
\r	Indicates a carriage return character.	(stress)**\r** matches any block of text that contained the substring “stress” followed immediately by one carriage return (ASCII 0x0D) character.

TABLE 6-10. Escape Sequences and Literal Strings (Continued)

ELEMENT	WHAT IT MEANS	EXAMPLE
\b	Indicates a backspace character. OR Denotes boundaries	(stress)**b** matches any block of text that contained the substring "stress" followed immediately by one backspace (ASCII 0x08) character. A word boundary (\b) is defined as a spot between two characters that has a \w on one side of it and a \W on the other side of it (in either order), counting the imaginary characters off the beginning and end of the string as matching a \W. (Within character classes \b represents backspace rather than a word boundary.) For example, the following regular expression can match the social security number: .REG. \b\d{3}-\d{2}-\d{4}\b
\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 characters preceded with a ~ (tilde) character. So, the words '~ab12cd', '~Pa3499' would be matched, but '~oops' would not.

Using Complex Expression Syntax

A keyword expression is composed of tokens, which is the smallest unit used to match the expression to the content. A token can be an operator, a logical symbol, or the operand, i.e., the argument or the value on which the operator acts.

Operators include .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., ".(." and " .)." The operand and the operator must be separated by a space. An operand may also contain several tokens. Refer to *Keywords* on page 6-23 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
```

Viewing Content Filtering Rules

Navigation Path: Security Settings > Messaging Security Agent > Configure > Content Filtering

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

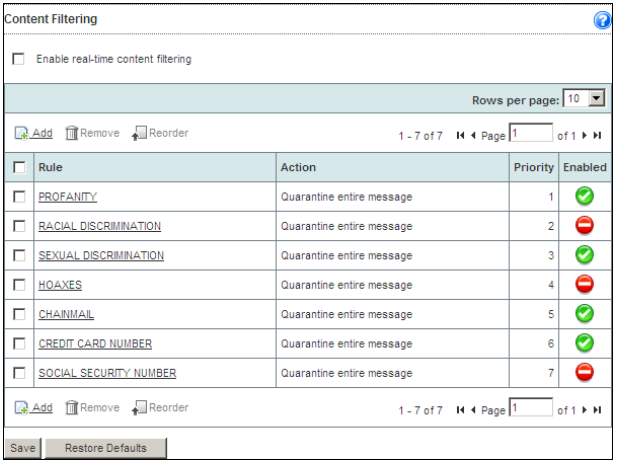


FIGURE 6-4. Content Filtering screen

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 6-39.
- **Reorder rules:** Refer to *Reordering Rules* on page 6-40.
- **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 Messaging Security Agent > 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**.
3. To filter messages that match any condition defined:
   a. Name the rule.
   b. Set the scan conditions.

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

d. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.

4. To filter messages that match all conditions defined:
   a. Name the rule.
   b. Set the scan conditions.
   c. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.
5. To monitor the message content of particular email accounts
   a. Name the rule.
   b. Set the accounts to monitor.
   c. Set the scan conditions.
   d. Add the keywords. Include synonyms and/or case-sensitive criteria.
   e. Configure the action on the message matching the criteria, set the people to be notified, archive the message, and/or set the replacement text or string.
6. To create an exception list for email accounts
   a. Name the rule.
   b. Set the accounts to exclude.

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

7. 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 Messaging Security Agent > 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.

TABLE 6-12. Attachment Blocking Actions (Continued)

Action	Description
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

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Attachment Blocking

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

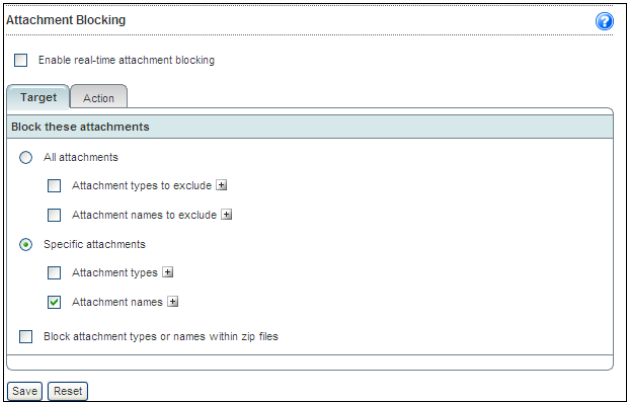


FIGURE 6-5. Attachment Blocking screen

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 6-42 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, WFBS-A will replace the threat with this text string and file.
3. Click **Save**.

Real-time Monitor

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Real-time Monitor

The Real-time Monitor displays current information about the selected Exchange Server and its Messaging Security Agent (MSA). It shows information about scanned messages and protection statistics, including the number of viruses and spam found, attachments blocked, and content violations.

The **Messaging Security Agent has been running since** field helps you verify whether the MSA is working properly.

To clear old information and start collecting fresh information in real time:

- Click **Reset** to reset the protection statistics to zero.
- Click **Clear Content** to clear older information about scanned messages.

To access the Real-time Monitor:

1. Click **Security Settings**.
2. Select an Exchange Server computer.
3. Click **Configure**.
4. Click the **Real-time Monitor** link on the upper right portion of the screen.

Messaging Agent 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 E-8.

Administrators can query the quarantine database to gather information about quarantined messages.

Use Quarantine to:

- Eliminate the chance of important messages being permanently deleted, if they are erroneously detected by aggressive filters
- Review messages that trigger content filters to determine the severity of the policy infraction

- Maintain evidence of an employee's possible misuse of the company's messaging system

Note: Do not confuse the quarantine folder with the end user's spam folder. The quarantine folder is a file-based folder. Whenever 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 WFBS-A, 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 Messaging Security Agent > Configure > Quarantine > Directory

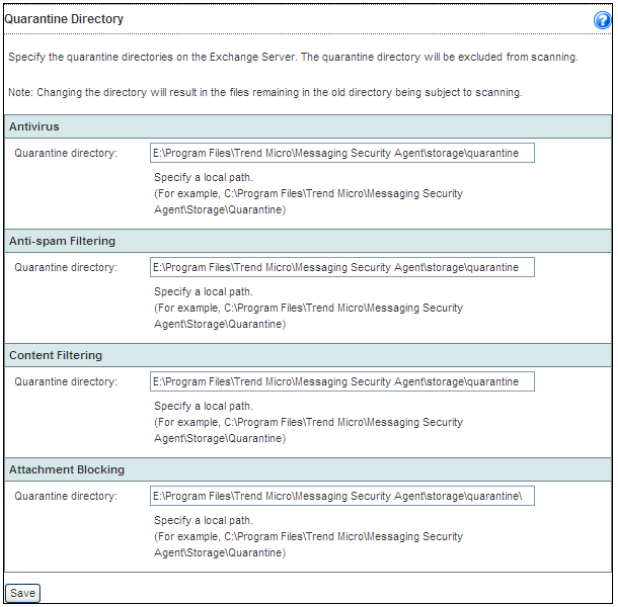


FIGURE 6-6. Quarantine Directory screen

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 6-46 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 Messaging Security Agent > Configure > Quarantine > Query

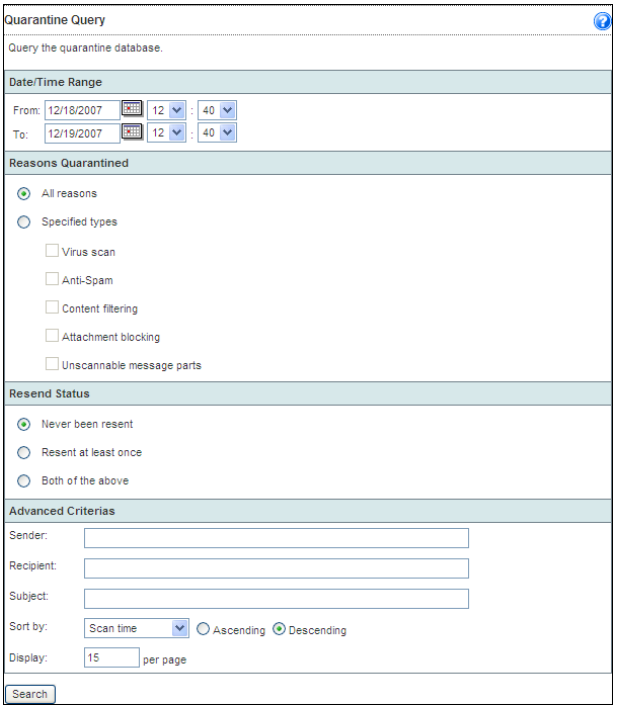


FIGURE 6-7. Quarantine Query screen

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 6-49 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 6-48.

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.**

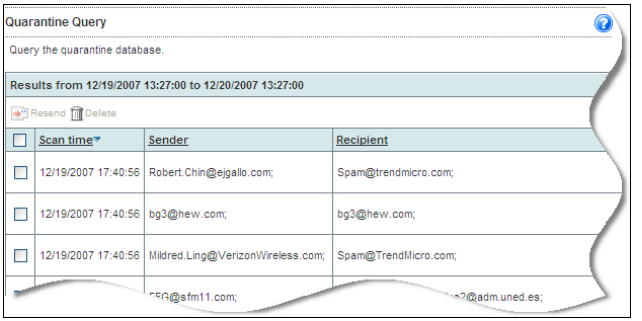


FIGURE 6-8. Quarantine Query Results screen

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 E-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.

Maintaining Quarantine Directories

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Quarantine > Maintenance

Use this feature to manually or automatically delete quarantined messages. This feature can delete all messages, messages that have been resent, messages that have not been resent.

FIGURE 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 *Spam Maintenance* on page 6-55.

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: WFBS-A 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.

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

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Operations > Notification Settings

WFBS-A can send notifications in the form of email messages to various alerts. Some notifications can be configured to apply to only internal email messages. Define the email addresses or domains to treat as internal addresses. Custom Internal Email Definitions are useful if your company has two or more domains and you would like to treat email messages from both domains as internal email messages. For example, example.com and example.net.

The recipients on your Internal Email Definitions list will receive messages for notifications when you select the **Do not notify external recipients** check box under the Notification settings for **Antivirus**, **Content Filtering**, and **Attachment Blocking**. Do not confuse the Internal Email Definitions list with the Approved Senders list.

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

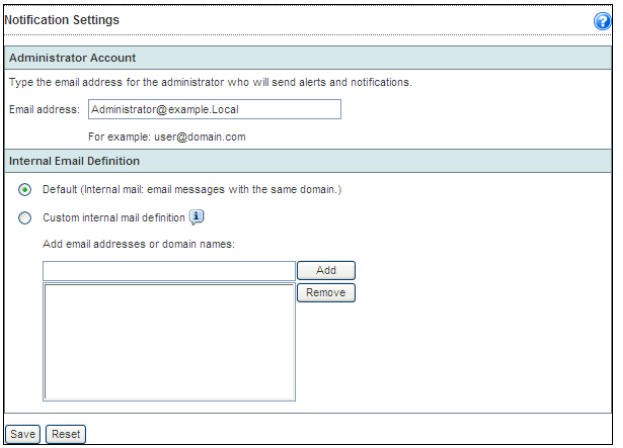


FIGURE 6-10. Notification Settings screen

To configure notification settings:

1. From the **Notification Settings** screen, update the following as required:
   - **Email address.** The address on behalf of whom WFBS-A will send notification messages.
   - **Internal Email Definition**
     - **Default:** WFBS-A will treat email messages from the same domain as Internal Emails.
     - **Custom:** Specify individual email addresses or domains to treat as internal email messages.
2. Click **Save**.

Spam Maintenance

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Operations > Spam Maintenance

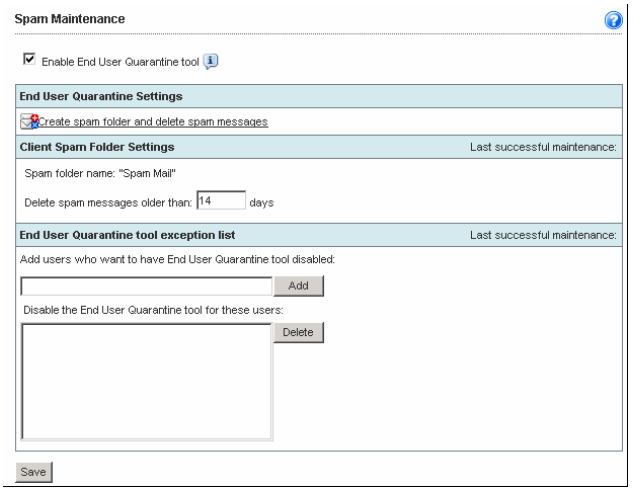


FIGURE 6-11. Spam Maintenance screen

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 *Managing POP3 Mail Scan* on page 5-26.

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
```

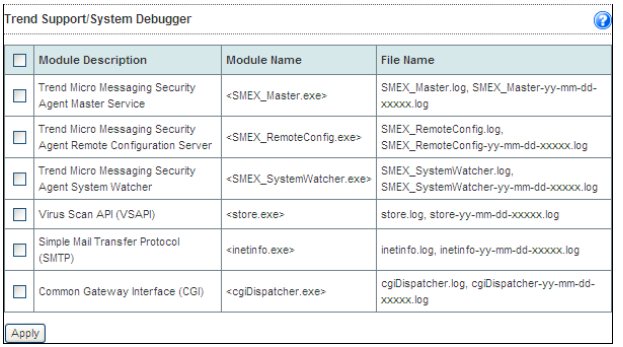
View the output with any text editor.

Generating System Debugger Reports

Navigation Path: Security Settings > Select a Messaging Security Agent > Configure > Operations > Trend Support/Debugger

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

To generate reports using the Debugger:


Trend Support/System Debugger

	Module Description	Module Name	File Name
☐	Trend Micro Messaging Security Agent Master Service	<SMEX_Master.exe>	SMEX_Master.log, SMEX_Master-yy-mm-dd-xxxxx.log
☐	Trend Micro Messaging Security Agent Remote Configuration Server	<SMEX_RemoteConfig.exe>	SMEX_RemoteConfig.log, SMEX_RemoteConfig-yy-mm-dd-xxxxx.log
☐	Trend Micro Messaging Security Agent System Watcher	<SMEX_SystemWatcher.exe>	SMEX_SystemWatcher.log, SMEX_SystemWatcher-yy-mm-dd-xxxxx.log
☐	Virus Scan API (VSAPI)	<store.exe>	store.log, store-yy-mm-dd-xxxxx.log
☐	Simple Mail Transfer Protocol (SMTP)	<inetinfo.exe>	inetinfo.log, inetinfo-yy-mm-dd-xxxxx.log
☐	Common Gateway Interface (CGI)	<cgiDispatcher.exe>	cgiDispatcher.log, cgiDispatcher-yy-mm-dd-xxxxx.log

Apply

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)
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**.

Adding Microsoft Exchange Servers to the Security Groups Tree

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

The Security Server provides a step-by-step wizard to help you Add, install or upgrade the Messaging Security Agent on a Microsoft Exchange server.

To add a Desktop or Microsoft Exchange Server:

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

Removing Microsoft Exchange Servers from the Web Console

You can use Remove to accomplish two goals:

- Remove the Microsoft Exchange server icon from the Web console
- In some situations, a Microsoft Exchange server might become inactive. In these situations, you might want to delete the Microsoft Exchange server icon from the Web console.

Uninstall the Messaging Security Agents from the Microsoft Exchange server (and consequently remove the Microsoft Exchange server icon from the Web console)

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

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

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

WARNING! Removing the Messaging Security Agent from a computer may expose that Microsoft Exchange server to viruses and other malware.

To remove a Microsoft Exchange server:

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

b. Select **Uninstall** to remove the Messaging Security Agent from the selected Microsoft Exchange server and remove the computer icons from the Web console.

   i. If necessary, type the account name and password for the Microsoft Exchange server that you want to remove.

   ii. Click **OK** from the warning message to complete the uninstallation.

3. Click **Next**.
4. Confirm your action by clicking **Apply**.

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

Replicating Settings for Microsoft Exchange Servers

To save time and maintain consistent security settings, you can replicate the settings from one Microsoft Exchange server to another.

To replicate settings:

1. From the Security Settings screen, choose the Microsoft Exchange server from which you want to replicate settings.
2. Click **Replicate**. The Security Settings > Replicate screen opens displaying the source you selected in the previous screen.
3. Select the target Microsoft Exchange server or server group to which you will replicate the settings.
4. Click **Apply**.

Note: You can only replicate settings from a source Microsoft Exchange server to a target Microsoft Exchange server that share the same domain.

Adding a Disclaimer to Outbound Email Messages

You can add a disclaimer message only to outgoing email messages.

To add a disclaimer to each outbound mail:

1. Create a text file and add the disclaimer text to this file.
2. Modify the following keys in the registry:
   - First key:

     Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion

     Key: EnableDisclaimer

     Type: REG_DWORD

     Data value: 0 - Disable, 1 - Enable

   - Second key:

     Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion

     Key: DisclaimerSource

     Type: REG_SZ

     Value: The full path of the disclaimer content file.

     For example, C:\Data\Disclaimer.txt

     Note: By default, WFBS-A will detect if an outbound mail is sent to the internal or external domains, and add a disclaimer to each mail sent to the external domains. The user can overwrite the default setting and add a disclaimer to each outbound mail except the domains included in the following registry key:

   - Third key:

     Path: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion

     Key: InternalDomains

     Type: REG_SZ

Value: Type the domain names to exclude. Use a semicolon (;) to separate multiple items.

For example: domain1.org;domain2.org

Note: The domain names here are the DNS names of the Exchange servers.

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

Outbreak Defense is a key component of WFBS-A 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

Outbreak Defense Current Status

Navigation Path: Outbreak Defense > Current Status

The Web console displays and tracks the status of a world-wide virus/malware outbreak threat on the **Current Status** screen. The status roughly corresponds to the outbreak life cycle.

During an outbreak, Outbreak Defense uses the Outbreak Defense Strategy to protect your computers and networks. In each stage, it refreshes the information in the Current Status page. The three stages of Outbreak Defense:

1. Threat Prevention
2. Threat Protection
3. Threat Cleanup

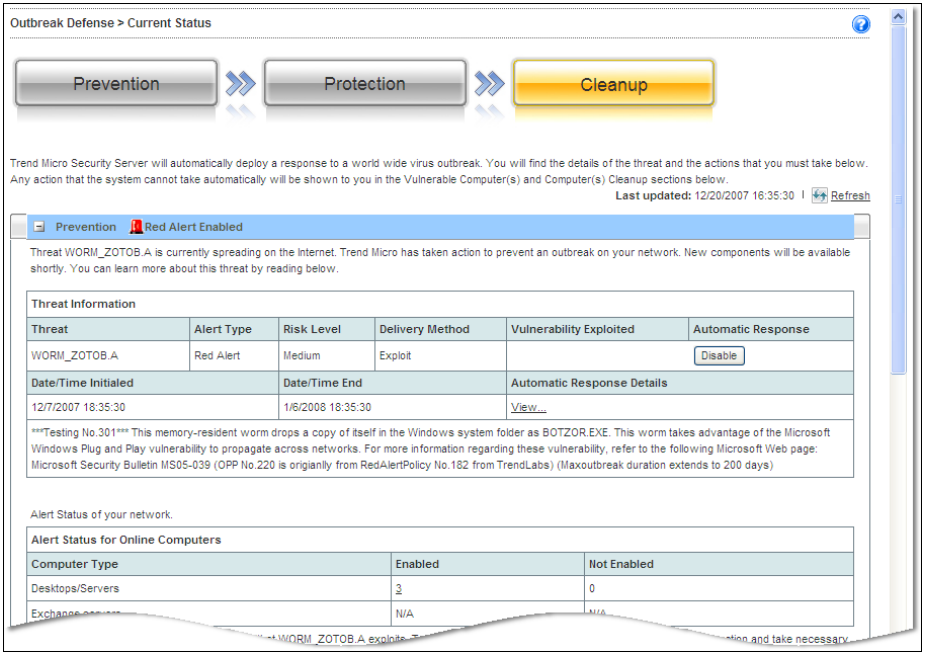


FIGURE 7-1. Outbreak Defense screen–No Threat

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.

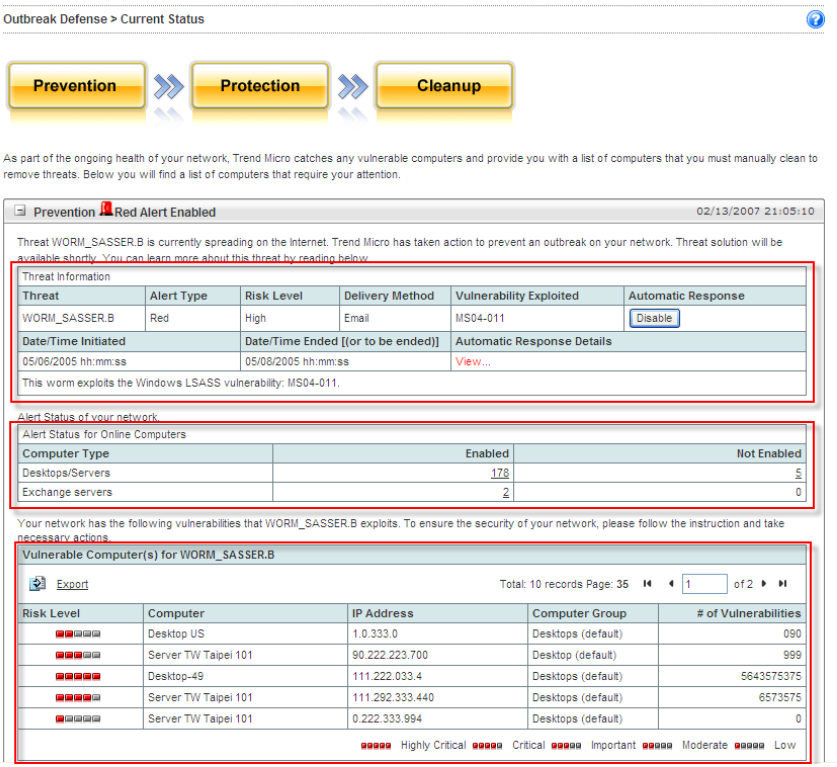


FIGURE 7-2. Outbreak Defense screen–Threat Prevention Stage

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 *Trend Micro Damage Cleanup Services* on page C-2).

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.

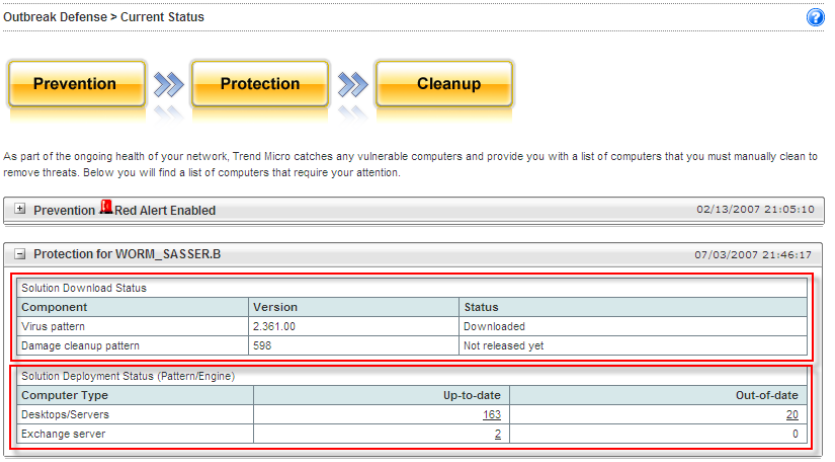


FIGURE 7-3. Outbreak Defense screen—Protection Stage

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.

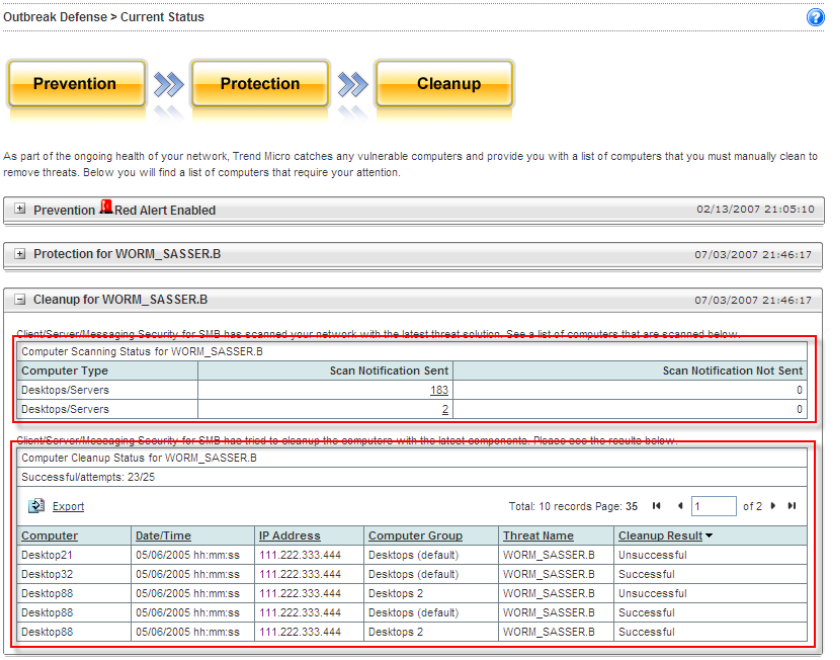


FIGURE 7-4. Outbreak Defense screen - Cleanup Stage

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.

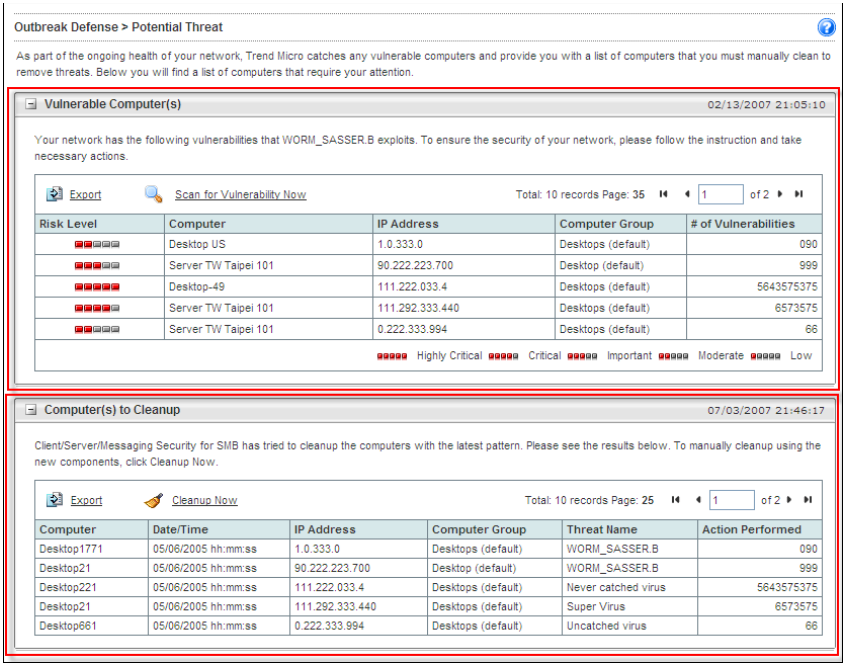


FIGURE 7-5. Potential Threat screen

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**, WFBS-A 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.

Running Cleanup Now

You can initiate a cleanup manually by running Cleanup Now.

To run Cleanup Now:

1. Click **Outbreak Defense > Potential Threat**.
2. Click the **Cleanup Now** link. By default, the Security Server notifies all agents to run Cleanup Now.

Setting up Outbreak Defense

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

Outbreak Defense Settings

WFBS-A 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

TABLE 7-2. Recommended Outbreak Defense Settings (Continued)

Setting	Recommended Value
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

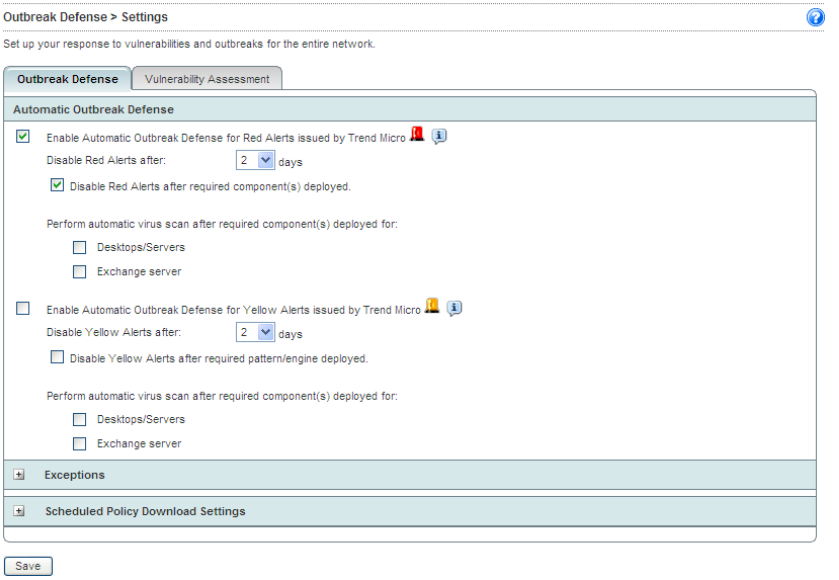


FIGURE 7-6. Outbreak Defense tab of Outbreak Defense Settings screen

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 7-11 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

Navigation Path: Outbreak Defense > Settings > Outbreak Defense tab

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

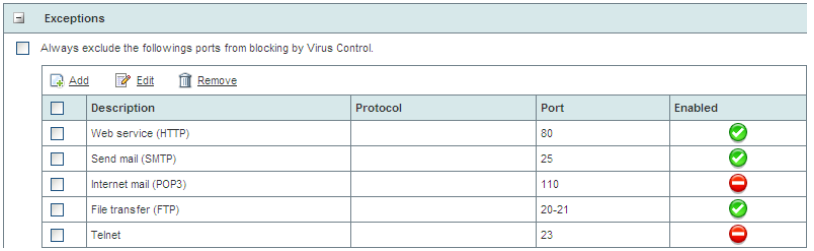


FIGURE 7-7. Exceptions section of Outbreak Defense Settings screen

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 it.

---

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

Viewing Automatic Outbreak Defense Details

Navigation Path: Outbreak Defense > Current Status > Prevention panel

During an outbreak, the Security Server activates Outbreak Defense. The Automatic Outbreak Defense prevents your computers and network from being damaged by the current outbreak during the critical time when TrendLabs is creating their solution to the current outbreak.

Automatic Outbreak Defense performs the following actions during a virus outbreak:

- Blocks shared folders to help prevent viruses from infecting files in shared folders
- Blocks ports to help prevent viruses from using vulnerable ports to infect files on the network and clients.

> **Note:** Outbreak Defense never blocks the port used by the Security Server to communicate with the clients.

- Denies write access to files and folders to help prevent viruses from modifying files
- Enables Attachment Blocking to block suspect attachment files
- Enables Content Filtering and creates a "Match All" or "Match Any" rule to filter threatening content

Configuring Vulnerability Assessment Settings

Navigation Path: Outbreak Defense > Settings > Vulnerability Assessment tab

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

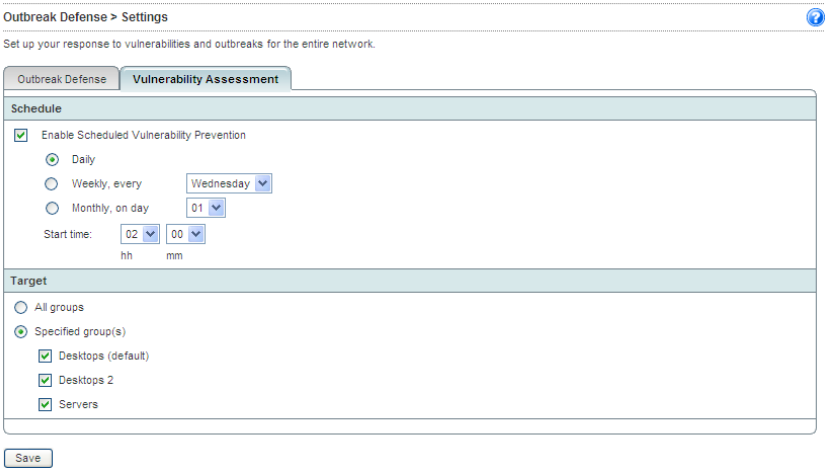


FIGURE 7-8. Vulnerability Assessment tab of Outbreak Defense Settings screen

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

Managing Scans

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

The topics discussed in this chapter include:

About Scanning

WFBS-A 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.

Scan Methods

Client Scanning is performed in two different ways:

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

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

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

Selecting the Scan Method

If client scans are slowing down client computers, consider switching to Smart Scan. By default, Smart Scan is enabled. You can disable Smart Scan for all clients on the **Preferences > Global Settings** screen under General Scan Settings.

To select the scan method:

1. Click **Security Settings** and click a server or desktop.
2. Click **Configure**.
3. On the top of the screen, click **Smart Scan** or **Conventional Scan**.

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

Scan Types

WFBS-A offers the following types of scans:

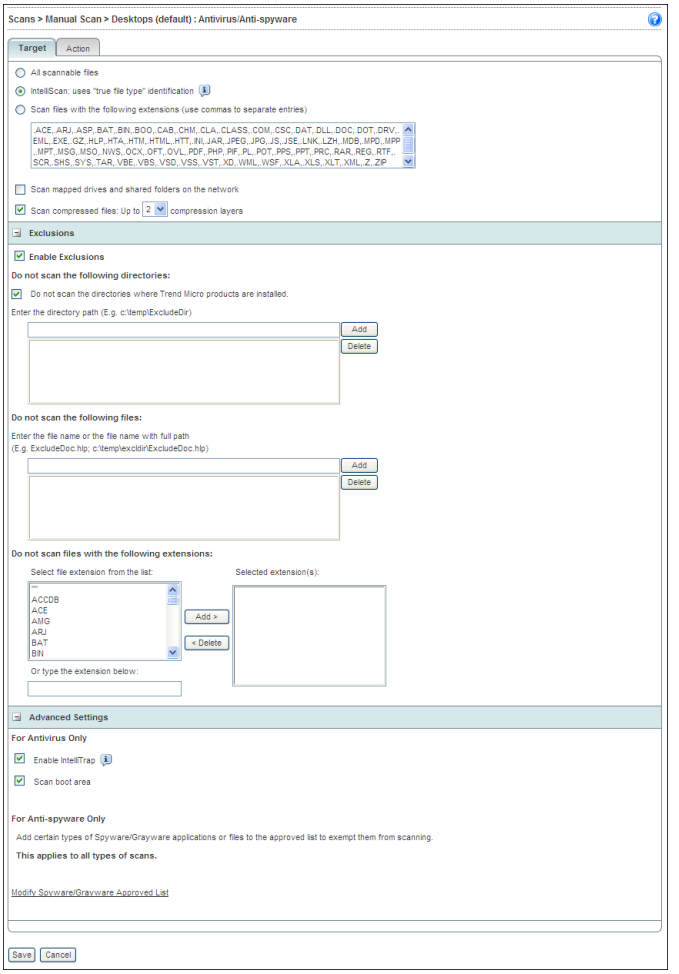
- Real-time Scan: an ongoing scan executed each time the client users download, save, copy, modify or open a file.
- Manual Scan: an on-demand scan that administrator or client users initiate.
- Scheduled Scan: a scan that starts at regular, scheduled times.

For more information, see *About Scan Types* on page 5-3.

Configuring Manual and Scheduled Scan Options

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

Navigation Path: Scans > Manual Scan or Scheduled Scan > 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:** WFBS-A 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 8-7 for more information.

2. From the **Action** tab, specify how WFBS-A 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:** WFBS-A 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 E-8
   - Action for Spyware/Grayware Detections
     - **Clean:** When cleaning spyware/grayware, WFBS-A 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 12-2 for more information.
3. Click **Save**.

   Additionally, configure who receives notifications when an event occurs.

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* on page 1-13 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 > Modify Spyware/Grayware Approved List

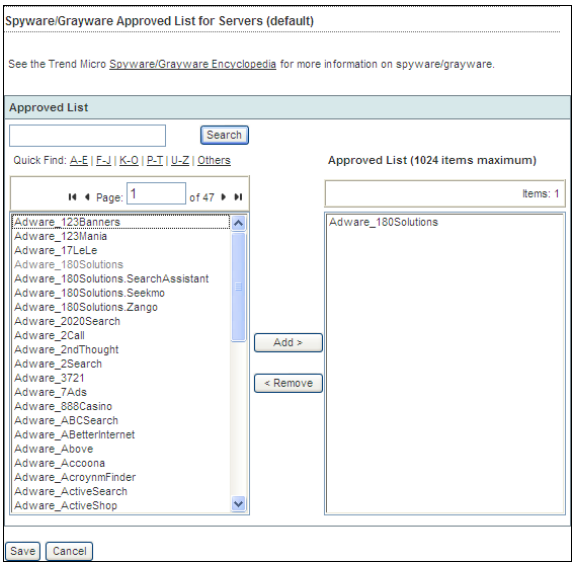


FIGURE 8-1. Spyware/Grayware Approved List screen

To update the Spyware/Grayware Approved List:

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

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

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

Configuring Scan Options for Microsoft Exchange Servers

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

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

3. For Scheduled Scans, update the schedule on the **Schedule** tab. Refer to *Scheduling Scans* on page 8-9.
4. Click **Scan Now** or **Save**.

Scheduling Scans

Navigation Path: Scans > Scheduled Scan > Schedule tab

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

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

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

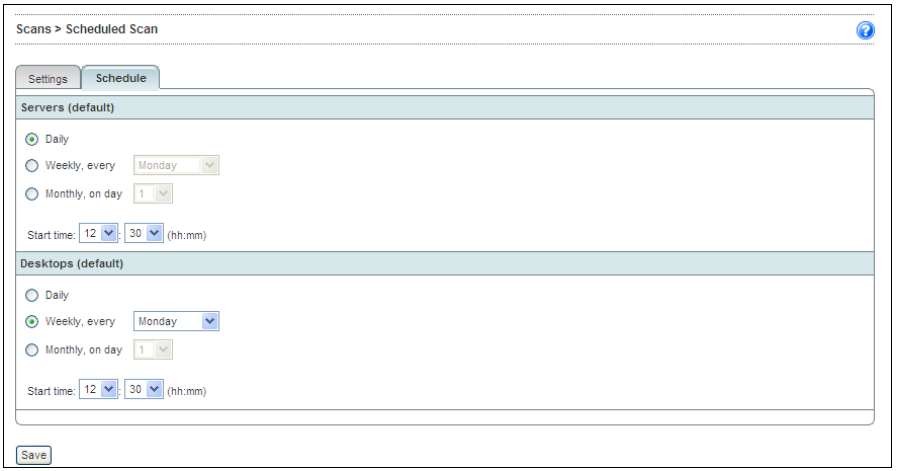


FIGURE 8-2. Scheduled Scan screen

To schedule a scan:

1. Before scheduling a scan, configure the settings for the scan. Refer to *Configuring Manual and Scheduled Scan Options* 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, WFBS-A 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 *Configuring Events for Notifications* on page 9-3.

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

Chapter 9

Managing Notifications

This chapter explains how to use the different notification options.

The topics discussed in this chapter include:

About Notifications

To minimize the amount of time Administrators need to monitor WFBS-A 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. WFBS-A 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).
- **Anti-spam:** Spam occurrences exceed a certain percentage of total email messages.
- **Web Reputation:** The number of URL violations exceeds the configured number in a certain period.
- **URL Filtering:** The number of URL violations exceeds the configured number in a certain period.
- **Behavior Monitoring:** The number of policy violations exceeds the configured number in a certain period.
- **Network Virus:** Network viruses detected exceeds a certain number.

System Events

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

License Events

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

Configuring Events for Notifications

Navigation Path: Preferences > Notifications > Events tab

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

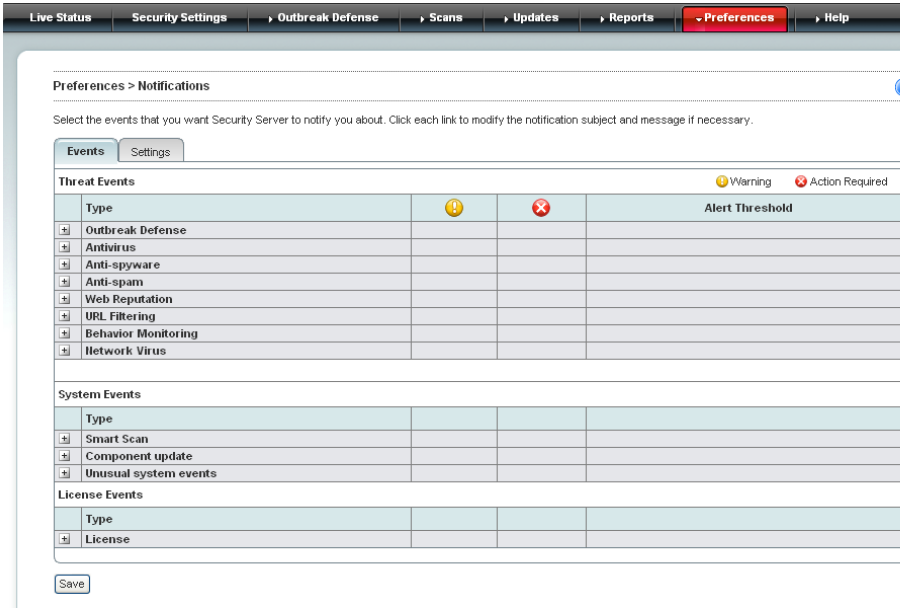


FIGURE 9-1. Notification Events screen

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

Navigation Path: Preferences > Notifications > Click a notification

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

The recipients on your Internal Email Definitions list will receive messages for notifications when you select the Do not notify external recipients check box under the Notification settings for Antivirus, Content Filtering, and Attachment Blocking. Do not confuse the Internal Email Definitions list with the Approved Senders list.

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

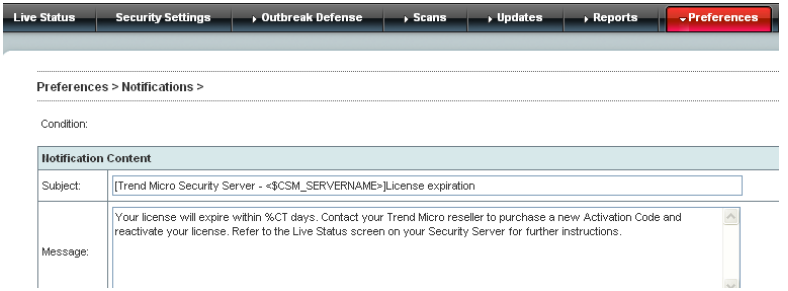


FIGURE 9-2. Notification content screen

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

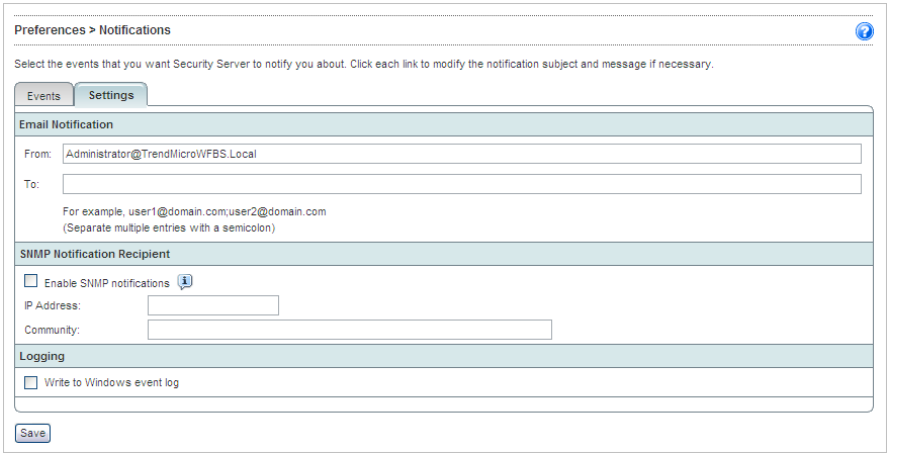


FIGURE 9-3 Notifications screen

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.**

Configuring Notification Settings for Microsoft Exchange Servers

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

Configure the From address for notifications and define internal mails.

To configure notification settings:

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

Chapter 10

Managing Global Settings

This chapter explains how to use Global Settings.

The topics discussed in this chapter include:

Configuring Global Preferences

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

Internet Proxy Options

Navigation Path: Preferences > Global Settings > Proxy tab

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

- Component updates and license notifications
- Web Reputation, Behavior Monitoring, Smart Feedback, Smart Scan, and URL Filtering.

You can use the same update proxy settings or enter new credentials.

Note: The agent will always use the same proxy server and port used by Internet Explorer to connect to the Internet for Web Reputation, behavior monitoring, and the Smart Protection Network. Duplicate the logon credentials you have specified for the update service only if Internet Explorer on client computers uses the same proxy server and port.

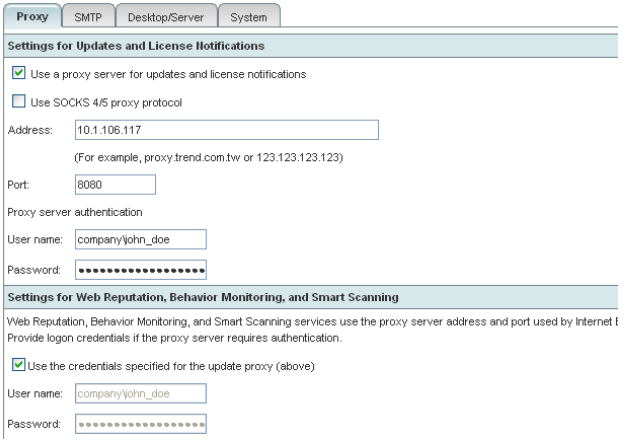


FIGURE 10-1. Global Settings–Proxy Server Settings screen

To configure Proxy Settings:

1. From the **Proxy** tab on the Global Settings screen, update the following as required:
   - **Settings for Updates and License Notifications**
     - **Use a proxy server for updates and license notifications**
     - **Address**
     - **Use SOCKS 4/5 proxy protocol**
     - **Port**
     - **Proxy server authentication**
       - **User name**
       - **Password**
   - **Settings for Web Reputation, Behavior Monitoring, and Smart Scanning**
     - **Use the credentials specified for the update proxy**
     - **User name**
     - **Password**
2. Click **Save**.

SMTP Server Options

The SMTP Server settings apply to all notifications and reports generated by WFBS-A.

Navigation Path: Preferences > Global Settings > SMTP tab

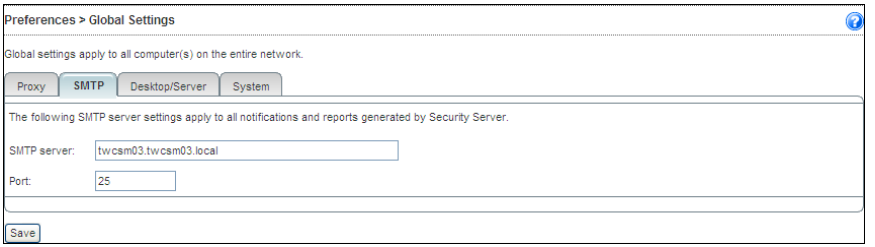


FIGURE 10-2. SMTP tab on the Global Settings screen

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

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

The Desktop/Server options pertain to the WFBS-A 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.

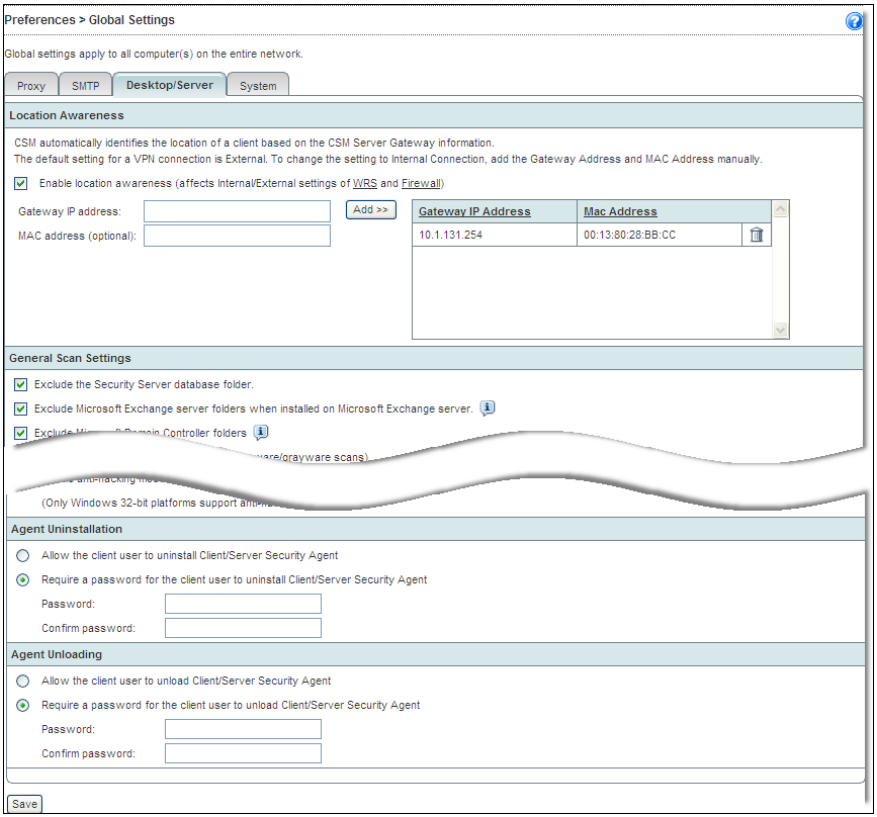


FIGURE 10-3. Desktop/Server tab of the Global Settings screen

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 10-6
   - *General Scan Settings* on page 10-7
   - *Virus Scan Settings* on page 10-7
   - *Spyware/Grayware Scan Settings* on page 10-8
   - *Approved URLs* on page 10-8
   - *Behavior Monitoring* on page 10-8
   - *IM Content Filtering* on page 10-9
   - *Alert Settings* on page 10-9
   - *Watchdog Settings* on page 10-10
   - *Agent Uninstallation* on page 10-10
   - *Agent Program* on page 10-10
2. Click **Save**.

Location Awareness

Location Awareness controls the In Office/Out of Office connection settings.

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

- **Enable location awareness:** These settings will affect the In Office/Out of Office connection settings of Firewall, Web Reputation, TrendSecure, and Smart Scan.
- **Gateway Information:** Clients and connections in this list will use Internal Connection settings while remotely connecting to the network (using VPN) and Location Awareness is enabled.
  - **Gateway IP address**
  - **MAC address:** Adding the MAC address improves security by permitting only the configured device to connect.

  Click the corresponding trash can icon to delete an entry.

General Scan Settings

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

- **Disable Smart Scan Service:** Switches all clients to Conventional Scan mode. Smart Scan will not be available until it is enabled again here.
- **Exclude the Security Server database folder:** Prevents agents installed on the Security Server from scanning its own database only during Real-time Scans.

Note: By default, WFBS-A 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.

Approved URLs

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

- **Enable the Approved URLs list**
- **Enable CSA usage logs:** Agents will send details of accessed URLs to the Security Server.
- **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 trash can icon.

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:

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

From the **Desktop/Server** tab of the **Global Settings** screen, use the following fields as described:

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

Alert Settings

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

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

Watchdog Settings

The Watchdog option ensures 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 without a password:** 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.

Agent Program

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

- **Allow client users to exit the agent program on their computer without a password:** Allows users to close the Client/Server Security Agent program.

- **Require client users to enter a password to exit the agent program:** Allows users to close the Client/Server Security Agent program after providing the specified password.

System Options

Navigation Path: Preferences > Global Settings > System tab

The System section of the Global Settings screen contains options to automatically remove inactive agents, check the connection of agents, and maintain the quarantine folder.

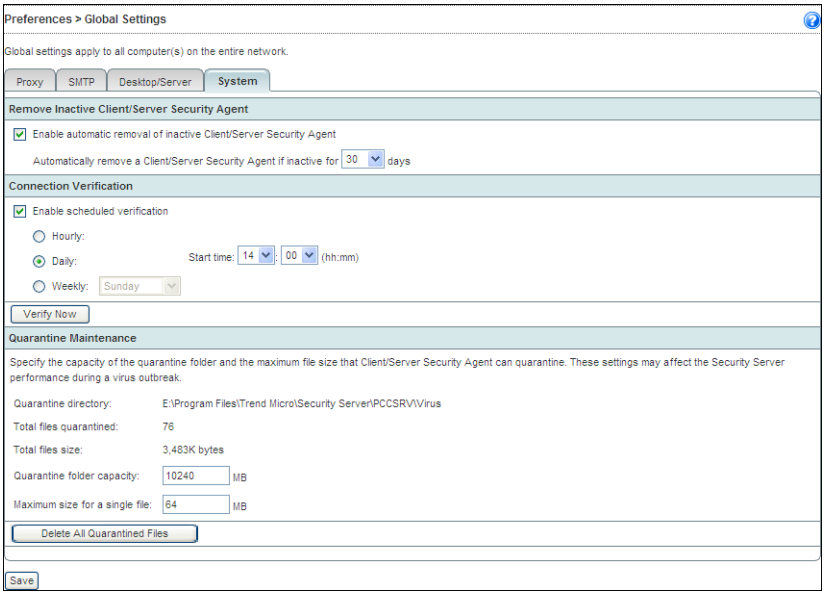


FIGURE 10-4. System tab of the Global Settings screen

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 10-12
   - *Verifying Client-Server Connectivity* on page 10-13
   - *Maintaining the Quarantine Folder* on page 10-13
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

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

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

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

To verify the client-server connectivity:

1. From the **System** tab of the **Global Settings** screen, update the following as required:
   - **Enable scheduled verification:** Enables scheduled verification of Agent-Security Server communication.
     - **Hourly**
     - **Daily**
     - **Weekly, every**
     - **Start time:** The time the verification should start.
   - **Verify Now:** Instantly tests the Agents-Security Server connectivity.
2. Click **Save.**

Maintaining the Quarantine Folder

Whenever an agent detects an Internet threat in a file and the scan action for that type of threat is quarantine, the agent encrypts the infected file, moves it to the client's quarantine folder, and sends it to the Trend Micro Security Server quarantine folder. WFBS-A 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 10-7.

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 11

Managing Updates

This chapter explains how to use and configure Manual and Scheduled Updates.

The topics discussed in this chapter include:

Updating Components

WFBS-A makes upgrading to the latest components easy by having agents automatically receive updated components from the Security Server.

WFBS-A downloads components from the Trend Micro ActiveUpdate Server:

- 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 WFBS-A 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 11-9). 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 WFBS-A

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 WFBS-A components regularly.

Configure the Security Server to download WFBS-A 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.

WFBS-A provides two methods for updating your components:

- Update your components manually, see *Manually Updating Components* on page 11-13.
- Update your components based on a schedule, see *Scheduling Component Updates* on page 11-14.

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 10-2.

TABLE 11-1. 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 Feedback engine 32-bit Feedback engine 64-bit Smart Scan Pattern Smart Scan Agent Pattern
Anti-spyware	Spyware scan engine 32-bit Spyware scan engine 64-bit Spyware pattern Spyware active-monitoring pattern
Anti-spam	Anti-spam pattern Anti-spam engine 32 -bit Anti-spam engine 64-bit
Web Reputation	URL filtering engine 32-bit URL filtering engine 64-bit

TABLE 11-1. Updatable Components (Continued)

COMPONENT	SUB-COMPONENT
Behavior Monitoring	Behavior Monitoring Driver Behavior Monitoring Core Service Policy Enforcement Pattern Digital Signature Pattern Behavior Monitoring Configuration Pattern Behavior Monitoring Detection Pattern
Outbreak Defense	Vulnerability pattern
Network Virus	Common firewall pattern Common firewall engine 32-bit Common firewall engine 64-bit Transport Driver Interface(TDI) driver 32-bit Transport Driver Interface(TDI) driver 64-bit WFP driver 32-bit WFP driver 64-bit

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

Default Update Times

By default, WFBS-A 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 WFBS-A 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 WFBS-A version. However, Trend Micro releases pattern files frequently.

Updating the Security Server

WFBS-A 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 WFBS-A 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 11-7.
2. Configure the Trend Micro Security Server for manual or scheduled updates. Refer to *Manual Updates* on page 11-12 and *Scheduled Updates* on page 11-14.
3. Use **Client Privileges** to configure update options for clients.

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 11-2. 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”.
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”.

TABLE 11-2. Update Source Options (Continued)

UPDATE OPTION	DESCRIPTION	RECOMMENDATION
ActiveUpdate server > Update Agents > Clients	Update Agents receive updated components directly from the Active-Update 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

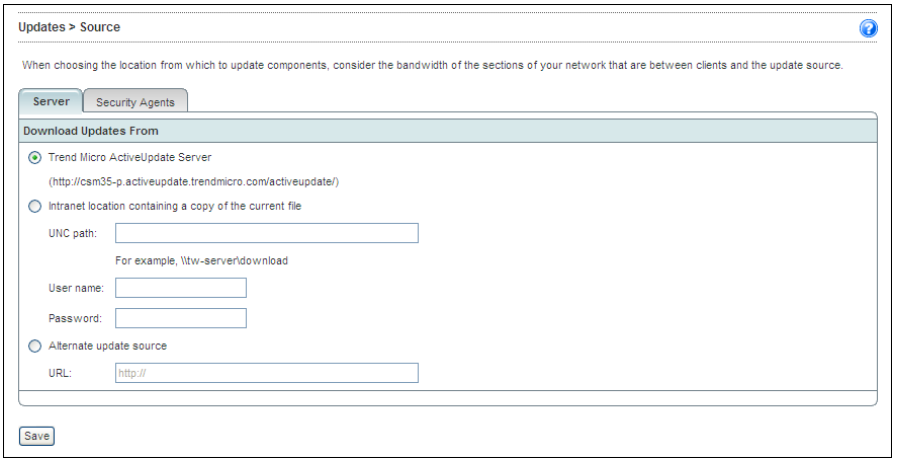


FIGURE 11-1. Update Source screen

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

Navigation Path: Updates > Source > Security Agents tab

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

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

To allow Agents to act as Update Agents:

1. From the **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 Updates

Navigation Path: Updates > Manual

The Security Server uses components to scan for and identify threats, and to perform damage cleanup tasks to help protect and clean the desktops and servers. It is essential to keep the components up-to-date. When you click **Update Now**, the Security Server searches for updated components. If updated components are available the Security Server downloads them and starts deploying them to clients.

The Manual Update screen contains the following items:

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

Manually Updating Components

Navigation Path: Updates > Manual Update

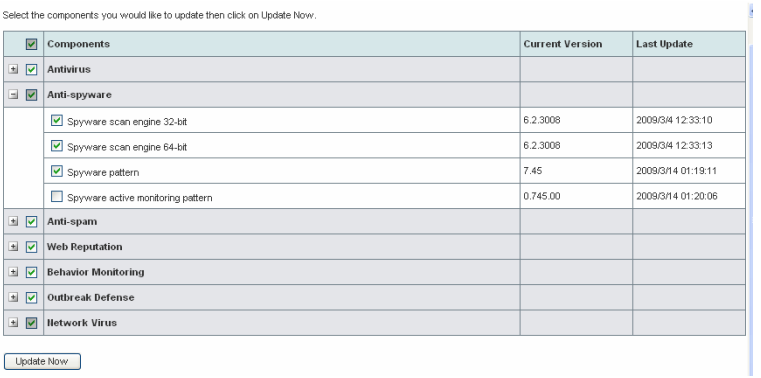


FIGURE 11-2. Manual Update screen

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 *Updatable Components* on page 11-3.
2. Click **Update Now** or **Save.** If scheduling updates, refer to *Scheduling Component Updates* on page 11-14.

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

Scheduled Updates

Navigation Path: Updates > Scheduled

The Security Server uses components to scan for and identify threats, and to perform damage cleanup tasks to help protect and clean the desktops and servers. It is essential to keep the components up-to-date. When you click Update Now, the Security Server searches for updated components. If updated components are available, the Security Server downloads them and starts deploying them to clients.

Scheduling Component Updates

Navigation Path: Updates > Scheduled Scan > Schedule tab

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.

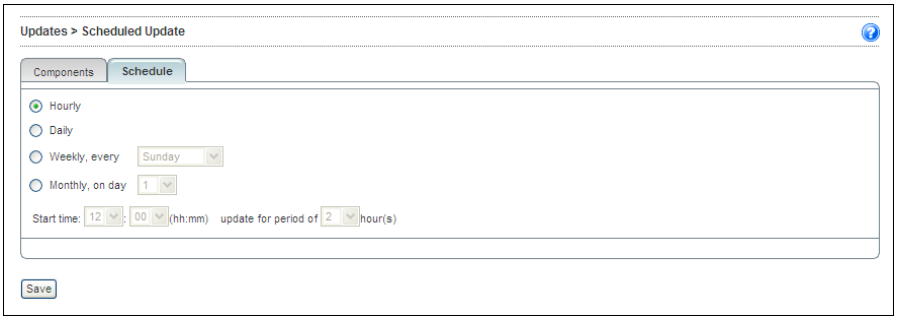


FIGURE 11-3. Scheduled Update screen

To schedule an update:

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

3. Click **Save**.

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

Rolling Back or Synchronizing Components

Navigation Path: Updates > Rollback

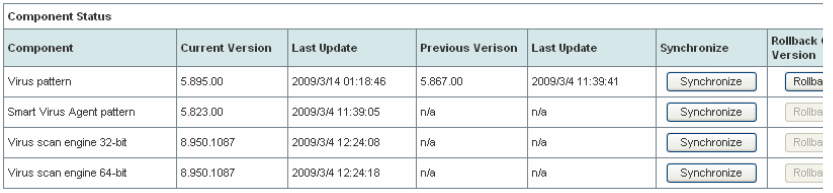
Rolling back refers to reverting to the previous version of a virus pattern file or scan engine. If the pattern file or scan engine that you are using is not functioning properly, roll back these components to their previous versions.

Synchronizing refers to deploying the updated components to all agents.

The agents use the following scan engines:

- Virus Pattern
- Smart Scan Agent Pattern
- 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.



Component Status

Component	Current Version	Last Update	Previous Verison	Last Update	Synchronize	Rollback Version
Virus pattern	5.895.00	2009/3/14 01:18:46	5.867.00	2009/3/4 11:39:41	Synchronize	Rollba
Smart Virus Agent pattern	5.823.00	2009/3/4 11:39:05	n/a	n/a	Synchronize	Rollba
Virus scan engine 32-bit	8.950.1087	2009/3/4 12:24:08	n/a	n/a	Synchronize	Rollba
Virus scan engine 64-bit	8.950.1087	2009/3/4 12:24:18	n/a	n/a	Synchronize	Rollba

FIGURE 11-4. 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.

Hot Fixes, Patches, and Service Packs

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

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

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

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

http://www.trendmicro.com/download

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

Chapter 12

Using Logs and Reports

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

The topics discussed in this chapter include:

Logs

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

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

WFBS-A maintains logs under the following categories:

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

TABLE 12-1. 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

TABLE 12-1. Log Type and Content (Continued)

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

Using Log Query

Navigation Path: Reports > Log Query

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

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

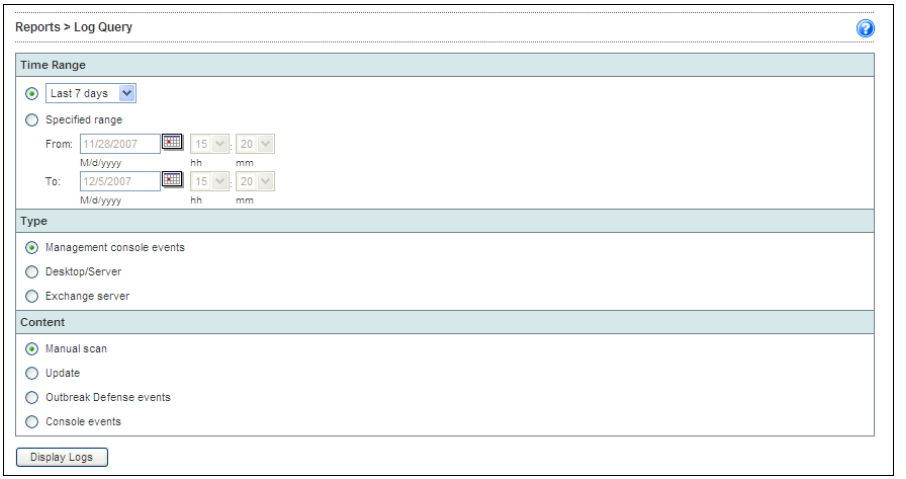


FIGURE 12-1. Default Log Query screen

To view logs:

1. From the **Log Query** screen, update the following options as required:
   - **Time Range**
     - **Preconfigured range**
     - **Specified range:** To limit the query to certain dates.

- **Type:** Refer to Table 12-1 on page 12-2 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.

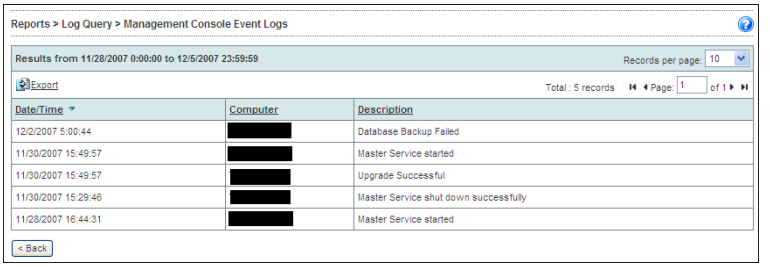


FIGURE 12-2. Sample Log Query screen

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, WFBS-A uses the template to generate the report.

Interpreting Reports

WFBS-A reports contain the following information. The information displayed could vary depending on the options selected.

TABLE 12-2. Contents of a Report

REPORT ITEM	DESCRIPTION
Antivirus	**Desktop/Servers Virus Summary** Virus reports show detailed information about the numbers and types of virus/malware that the scan engine detected and the actions it took against them. The report also lists the Top virus/malware names. Click the names of the virus/malware to open a new Web browser page and redirect it to the Trend Micro virus encyclopedia to learn more about that virus/malware. **Top 5 Desktop/Servers with Virus Detections** Displays the top five desktops or servers reporting virus/malware detections. Observing frequent virus/malware incidents on the same client might indicate that a client represents a high security risk that might require further investigation
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).

TABLE 12-2. Contents of a Report (Continued)

REPORT ITEM	DESCRIPTION
Anti-spyware	**Desktop/Servers Spyware/Grayware Summary** The spyware/grayware report shows detailed information about the spyware/grayware threats detected on clients, including the number of detections and the actions that WFBS-A 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.
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.
Web Reputation	**Top 10 Computers Violating Web Reputation Policies** Lists the top 10 clients that have violated Web Reputation policies.
URL category	**Top 5 URL Category Policies Violated** Lists the most commonly accessed Web site categories that violated the policy. **Top 10 Computers Violating URL Category Policies** Lists the top 10 computers that violated the URL Filtering policy.

TABLE 12-2. Contents of a Report (Continued)

REPORT ITEM	DESCRIPTION
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.
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. **Top 10 Computers Attacked** List the computers on your network that report the most frequent virus incidents.

Generating Reports

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

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

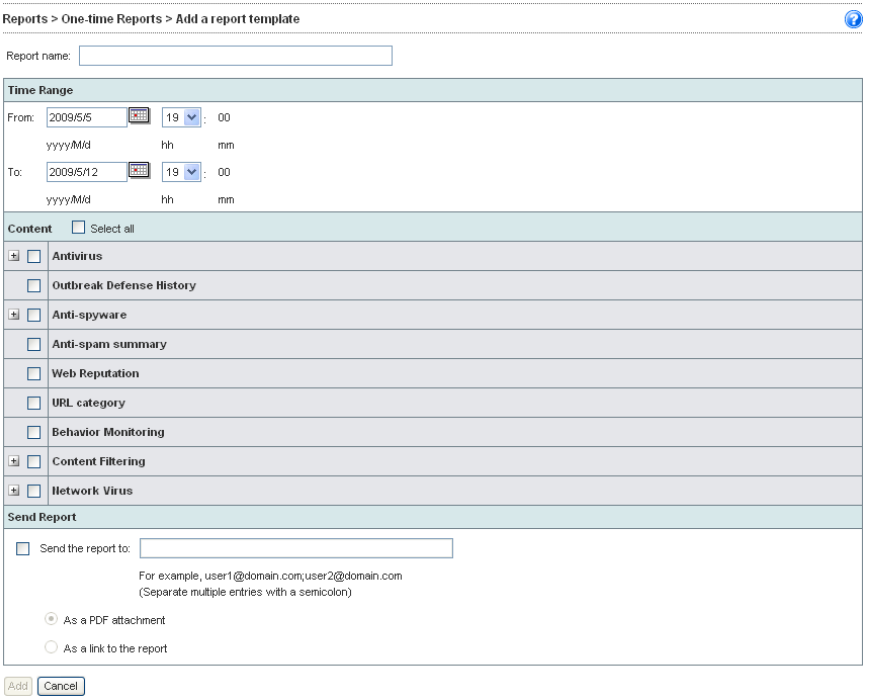


FIGURE 12-3. Reports screen

To create or schedule a report:

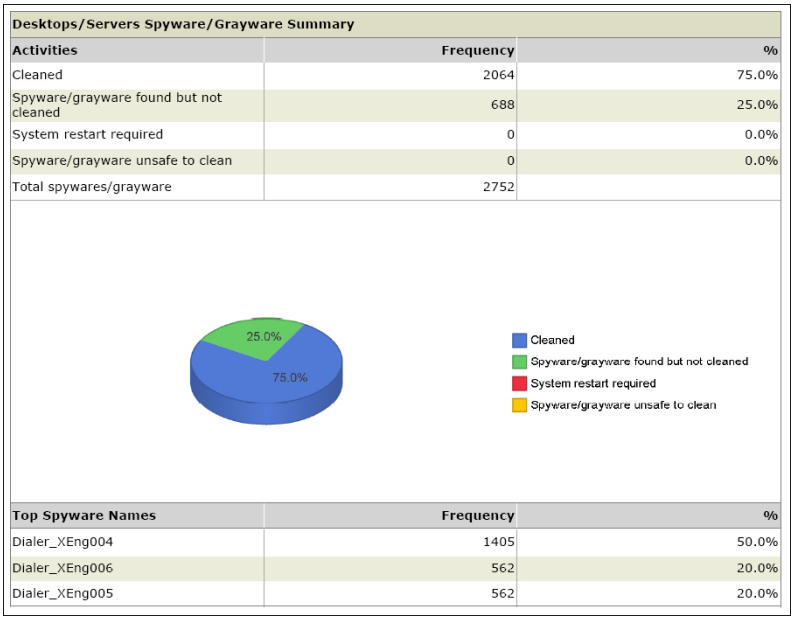
1. From the **One-time Reports** screen or **Scheduled Report** screen, click **Add**.
2. Update the following options as required:
   - **Report Name/Report Template Name:** A brief title that helps identify the report/template.

- **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, WFBS-A will not generate the report that month.
  - **Generate report at:** The time WFBS-A should generate the report.
- **Time Range:** Limits the report to certain dates.
- **Content:** To select all threats, select the **Select All** check box. To select individual threats, click the corresponding check box. Click  to expand the selection.
- **Send the report to:** WFBS-A 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, WFBS-A 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 12-4. 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. WFBS-A allows you to automate this task. Reports are based on logs, and, when the log information is deleted, reports can no longer be generated.

Maintaining Reports

Navigation Path: Reports > Maintenance > Reports tab

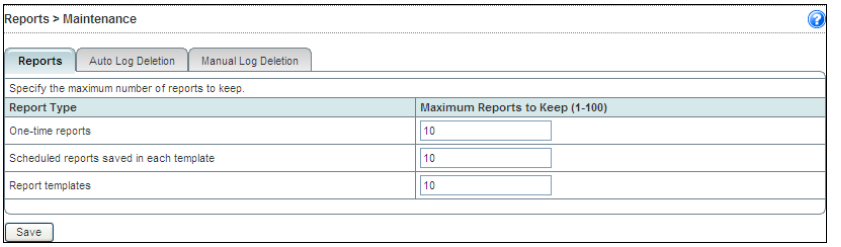


FIGURE 12-5. Reports Maintenance screen

Reports can accumulate quickly if not deleted. Deleting reports can be a time-consuming and tedious task. Worry-Free Business Security allows you to automate this task. Reports are based on logs. When the log information is deleted, reports can no longer be generated. From here you can:

Maintain Reports

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 Delete Logs

To automatically delete logs:

1. From the **Auto Log Deletion** tab on the Maintenance screen, select the **Log Type** and specify the number of days to store them.
2. Click **Save**.

Manually Delete Logs

To manually delete logs:

1. From the **Manual Log Deletion** tab on the Maintenance screen, specify the number of days to store a log type and click **Delete** corresponding to the log type.
2. Click **Save**.

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

Deleting Logs

Use the Reports > Maintenance screen to set up how long to keep log files and to schedule regular log maintenance.

Navigation Path: Reports > Maintenance > Auto Log Deletion tab

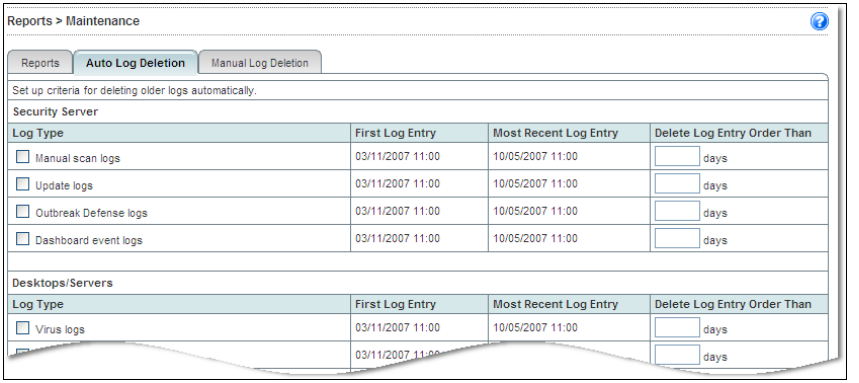


FIGURE 12-6. Auto Log Deletion screen

To set the Security Server to delete logs that exceed a set time limit:

1. Click **Reports > Maintenance**.
2. Click **Auto Log Deletion**.
3. Select the logs you want to delete.

4. In **Delete Logs Older Than**, type the number of days you want to the Security Server to retain logs.
5. Click **Save**. The Security Server will delete all logs older than the number of days you specified in step 4.

To manually delete a log:

1. Click **Manual Log Deletion**.
2. Find the row which displays the type of log to delete. Type a number in the field next to days to indicate a time limit.
3. Click **Delete**. All logs older than the amount of days you specified in step 2 are deleted.

Chapter 13

Administering WFBS-A

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

To prevent unauthorized users from modifying your settings or removing the agent from your clients, the Web console is password protected. The WFBS-A 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

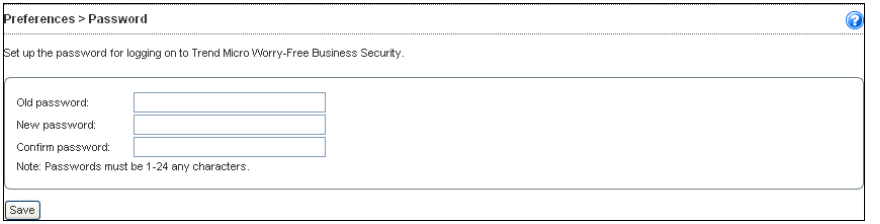


FIGURE 13-1. Preferences–Password screen

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 WFBS-A. Refer to *Uninstalling the Trend Micro Security Server* on page 13-7.

Working with the Plug-in Manager

Navigation Path: Preferences > Plug-ins

Plug-in Manager displays the programs for both the WFBS-A 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

Navigation Path: Preferences > Product License

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

FIGURE 13-2. Preferences–Product License screen

The Product License screen displays details about your license. Depending on the options you chose during installation, you might have a fully licensed version or an evaluation version. In either case, your license entitles you to a maintenance agreement. When your maintenance agreement expires the clients on your network will be protected in a very limited way. Use the Product License screen to determine when your license will expire and ensure that you renew your license before it expires.

Consequences of an Expired License

When a Full-version Activation Code expires, you can no longer perform important tasks, such as downloading updated components or using Web Reputation, etc. However, unlike an evaluation-version Activation Code, when a full-version Activation Code expires, all existing configurations and other settings remain in force. This provision maintains a level of protection in case you accidentally allow your license to expire.

To renew the product license:

1. Contact your Trend Micro sales representative or corporate reseller to renew your license agreement.

   Reseller Information stored in:

   ```
   Program files\trend micro\security server\pccsrv\
   private\contact_info.ini
   ```

2. A Trend Micro representative will update your registration information using Trend Micro Product Registration.
3. The Security Server polls the Product Registration server and receives the new expiry date directly from the Product Registration server. You are not required to manually enter a new Activation Code when renewing your license.

Changing your License

Your Activation Code determines the type of license you have. You might have an evaluation or a fully licensed version; or you might have a Worry-Free Business Security Advanced license or a Worry-Free Business Security License. If you want to change your license, you can use the Product License screen to enter a new Activation Code.

To change your license from an evaluation version to a fully licensed version:

1. Click **Enter a new code.**
2. Type your new Activation Code in the space provided.
3. Click **Activate.**

Participating in the Smart Protection Network

Navigation Path: Preferences > Smart Protection Network

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

- File checksums
- Web addresses accessed

- File information, including sizes and paths
- Names of executable files

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

For more information on the Smart Protection Network, visit:

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

To enable Trend Micro Smart Feedback:

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

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 also uninstalls the Scan Server.

WFBS-A 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 3-20.

To remove the Trend Micro Security Server:

1. On the computer you used to install the server, click **Start** > **Control Panel** > **Add or Remove Programs**.
2. Click **Trend Micro Security Server**, and then click **Change/Remove**. A confirmation screen appears.
3. Click **Next**. Master Uninstaller, the server uninstallation program, prompts you for the Administrator password.
4. Type the Administrator password in the text box and click **OK**. Master Uninstaller then starts removing the server files. A confirmation message appears after Security Server has been uninstalled.
5. Click **OK** to close the uninstallation program.

Appendix A

Trend Micro Product Exclusion List

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

TABLE A-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=

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

PRODUCT NAME	INSTALLATION PATH LOCATION
InterScan Web Security Suite (IWSS)	HKEY_LOCAL_MACHINE\Software\Trend-Micro\Interscan Web Security Suite Program Directory= C:\Program Files\Trend Mircro\IWSS
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFT-WARE\TrendMicro\InterScan WebPro-tect\CurrentVersion ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFT-WARE\TrendMicro\ InterScan FTP Virus-Wall\CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFT-WARE\TrendMicro\ InterScan Web Virus-Wall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFT-WARE\TrendMicro\ InterScan E-Mail Virus-Wall\CurrentVersion ProgramDirectory={Installation Drive}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFT-WARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFT-WARE\TrendMicro\ InterScan E-Mail Virus-Wall \CurrentVersion ProgramDirectory=

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

PRODUCT NAME	INSTALLATION PATH LOCATION
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 A-1. Trend Micro Product Exclusion List (Continued)

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=

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

PRODUCT NAME	INSTALLATION PATH LOCATION
ScanMail for Microsoft Exchange (SMEX) Continued	Get exclusion.txt file path from HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir Go to HomeDir path (for example, C:\Program Files\Trend Micro\Messaging Security Agent\) Open exclusion.txt C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

Exclusion List for Microsoft Exchange Servers

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\CurrentVersion\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 B

Client Information

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

The topics discussed in this appendix include:

Types of Clients

WFBS-A 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.

Normal Client Icons

Conventional Scan Client Status: Normal

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

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

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

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

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

If the following icons appear, verify that the Security Server is running and your clients are connected to your network.

TABLE B-2. Icons for Clients Disconnected from the Security Server (Conventional Scan)

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

Conventional Scan Client Status: Real-time Scan Not Operational

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

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

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

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

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

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

Smart Scan Client Status: Normal

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

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

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

Smart Scan Client Status: Disconnected from Smart Scan Server

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

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

Icon	Description
	Disconnected from the Scan Server but connected to the Security Server
	Disconnected from the Scan Server and also disconnected from the Security Server

Smart Scan Client Status: Real-time Scan not Operational

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

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

Icon	Description
	Real-time Scan is disabled but the client is connected to the Scan Server and the Security Server
	Real-time Scan is disabled, the client is connected to the Scan Server, but not the Security Server
	Real-time Scan is disabled, the client is not connected to the Scan Server but is connected to the Security Server
	Real-time Scan is disabled and the client is not connected to either the Scan Server or the Security Server

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

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

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

Location Awareness

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

WFBS-A automatically identifies the location of the client based on the Worry-Free Business Security Server Gateway information and controls the Web sites users can access. The restrictions differ based on the user's location:

- **Normal Clients** are computers that are stationary and maintain a continuous network connection with the Security Server.
- **Roaming Clients** are computers that do not always maintain a constant network connection

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 5-28.

The status of a Roaming Client is indicated by icons that appear in its system tray. Refer to the following tables for a list of icons that appear on Roaming Clients.

TABLE B-9. Icons that Appear on a Roaming Client (Conventional Scan)

ICON	DESCRIPTION
	Roaming Client (blue icon)
	Real-time Scan is disabled
	Pattern file is outdated
	Real-time Scan is disabled and the pattern file is outdated
	Real-time Scan Service is not running (red icon)
	Real-time Scan Service is not running and the pattern file is outdated (red icon)
	Connected to the Smart Scan Server but Real-time Scan is not operational
	Connected to the Smart Scan Server but Real-time Scan is disabled

TABLE B-9. Icons that Appear on a Roaming Client (Conventional Scan)

ICON	DESCRIPTION
	Not connected to the Smart Scan Server
	Not connected to the Smart Scan Server and Real-time Scan is not operational
	Not connected to the Smart Scan Server and Real-time Scan is disabled

TABLE B-10. Icons that Appear on a Roaming Client (Smart Scan)

ICON	DESCRIPTION	SCAN SERVER CONNECTION
	Roaming Client	Connected
	Roaming Client	Disconnected
	Real-time Scan disabled	Connected
	Real-time Scan disabled	Disconnected
	Real-time Scan Service is not running (red icon)	Connected
	Real-time Scan Service is not running (red icon)	Disconnected

32-bit and 64-bit Clients

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

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

Appendix C

Trend Micro Services

This appendix explains the services that Trend Micro offers.

The topics discussed in this appendix include:

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

WFBS-A 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 WFBS-A, 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 WFBS-A service is restarted (the WFBS-A 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 10-10 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, WFBS-A 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 C-1. Default ActiveAction Settings

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

Note: Future pattern files could update the default actions.

Trend Micro IntelliTrap

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

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

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

True File Type

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

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

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

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

Trend Micro 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 WFBS-A 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 Reputation

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

If Web Reputation blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list. For information on adding a URL to the Approved URL list, see Configuring Global Settings.

Reputation Score

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

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

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

Appendix D

Best Practices for Protecting Your Clients

This appendix provides you with some best practices that help you better protect the clients on your network.

Best Practices

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

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

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

  Trend Micro recommends requiring Web browsers to prompt users before installing ActiveX controls. To increase the security level for Internet Explorer (IE), go to **Tools** > **Internet Options** > **Security** and move the slider to a higher level. If this setting causes problems with Web sites you want to visit, click **Sites...**, and add the sites you want to visit to the trusted sites list.
- If using Microsoft Outlook, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages.
- Prohibit the use of peer-to-peer file-sharing services. Internet threats may be masked as other types of files your users may want to download, such as MP3 music files.

- Periodically examine the installed software on the computers on your network. If you find an application or file that WFBS-A cannot detect as an Internet threat, send it to Trend Micro:

  http://subwiz.trendmicro.com/SubWiz

  TrendLabs will analyze the files and applications you submit.

  If you prefer to communicate using email, send a message to the following address:

  virusresponse@trendmicro.com

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

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

Appendix E

Using Administrative and Client Tools

This appendix explains how to use the administrative and client tools that come with WFBS-A.

The topics discussed in this appendix include:

Tool Types

WFBS-A 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 WFBS-A.
  - **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 WFBS-A 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 WFBS-A are not available in this version. If you require these tools, contact Trend Micro Technical Support. Refer to *Technical Support* on page G-3

Administrative Tools

This section contains information about WFBS-A 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 3-6.

Vulnerability Scanner

Use Vulnerability Scanner to detect installed antivirus solutions and to search for unprotected computers on your network. To determine if computers are protected, Vulnerability Scanner pings ports that are normally used by antivirus solutions.

Vulnerability Scanner can perform the following functions:

- Perform a DHCP scan to monitor the network for DHCP requests so that when computers first log on to the network, Vulnerability Scan can determine their status
- Ping computers on your network to check their status and retrieve their computer names, platform versions, and descriptions
- Determine the antivirus solutions installed on the network. It can detect Trend Micro products (including OfficeScan, ServerProtect™ for Windows NT and Linux, ScanMail for Microsoft Exchange, InterScan Messaging Security Suite, and PortalProtect) and third-party antivirus solutions (including Norton AntiVirus Corporate Edition v7.5 and v7.6, and McAfee VirusScan ePolicy Orchestrator).
- Display the server name and the version of the pattern file, scan engine and program for OfficeScan and ServerProtect for Windows NT
- Send scan results through email

- Run in silent mode (command prompt mode)
- Install the Client/Server Security Agent remotely on computers running Windows 2000/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 WFBS-A 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 WFBS-A.

Using the Vulnerability Scanner

To configure Vulnerability Scanner:

1. In the drive where you installed the server component of WFBS-A, 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 E-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`.

Remote Manager Agent

The Trend Micro™ Worry-Free™ Remote Manager Agent allows resellers to manage WFBS-A with Trend Micro Worry-Free Remote Manager (WFRM). See the WFBS-A Installation Guide or the WFRM documentation for details.

Client Tools

This section contains information about WFBS-A 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. WFBS-A 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

Using the Graphical Interface

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

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

Using the Command Line Interface

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

1. Copy VSEncrypt from the Security Server to the client:
   \PCCSRV\Admin\Utility\VSEncrypt.

WARNING! Do not copy the VSEncrypt **folder to the WFBS folder. The** VSAPI32.dll **file of Restore Encrypted Virus will conflict with the original** VSAPI32.dll**.**

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

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

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

Restore Encrypted Virus provides the following logs:

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

To encrypt or decrypt files in other locations:

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

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

Restoring Transport Neutral Encapsulation Format Email Messages

Transport Neutral Encapsulation Format (TNEF) is a message encapsulation format used by Microsoft Exchange/Outlook. Usually this format is packed as an email attachment named Winmail.dat and Outlook Express hides this attachment automatically. Refer to

http://support.microsoft.com/kb/241538/en-us

If MSA archives this kind of email, and the extension of the file is changed to .EML, Outlook Express will only display the body of the email message.

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 WFBS-A 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 WFBS-A server on the network, you can use Client Mover to transfer clients from one WFBS-A server to another.

This is especially useful after adding a new WFBS-A server to the network when you want to transfer existing clients to the new server. Source and destination servers must be running the same version of WFBS-A and operating systems.

Client Mover requires the IpXfer.exe file.

To run Client Mover:

1. On the WFBS-A 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 WFBS-A server (the server to which the client will transfer)
   - <server_listening_port> = the listening (trusted) port of the destination WFBS-A 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

WFBS-A 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.

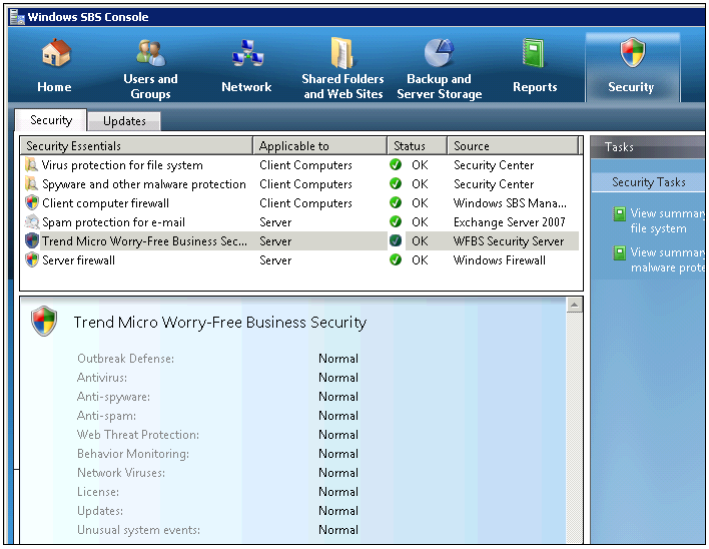


FIGURE E-1. SBS console displaying Live Status information

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.

Appendix F

Troubleshooting and Frequently Asked Questions

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

The topics discussed in this appendix include:

Troubleshooting

This section helps you troubleshoot issues that may arise while installing or using WFBS-A

Environments with Restricted Connections

If your environment has restrictions connecting to the Internet, in the case of a closed LAN or lack of an Internet connection, use the following procedures:

If Agents can access the Security Server:

1. Create a new package using the Client Packager (*Installing with Client Packager* on page 3-8).
2. Manually install the package on the computer.

The agent now applies the security settings as configured on the server.

If Agents cannot access the Security Server:

1. Create a new package using the Client Packager.
2. Manually install the package on the computer.

Client Packager Post-Installation Problems

If you installed the agent with Client Packager and are encountering problems, consider the following:

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

User's Spam Folder not Created

When the Administrator creates a mailbox account for a user, the spam folder is not created immediately in Microsoft Exchange server, but will be created under the following conditions:

- An end user logs on to their mailbox for the first time
- The first email arrives at the mailbox

The Administrator must first create the mailbox entity and the user must log on before EUQ can create a spam folder.

Internal Sender-Recipient Confusion

You can only define one domain as the internal address for the Messaging Security Agent. If you use Microsoft Exchange System Manager to change your primary address on a server, Messaging Security Agent does not recognize the new address as an internal address because Messaging Security Agent cannot detect that the recipient policy has changed.

For example, you have two domain addresses for your company: @example_1.com and @example2.com. You set @example_1.com as the primary address. Messaging Security Agent considers email messages with the primary address to be internal (that is, abc@example_1.com, or xyz@example_1.com are internal). Later, you use Microsoft Exchange System Manager to change the primary address to @example_2.com. This means that Microsoft Exchange now recognizes addresses such as abc@example_2.com and xyz@example_2.com to be internal addresses.

Re-sending a Quarantine Message Fails

This can happen when the system administrator's account on the Microsoft Exchange server does not exist.

To resolve quarantined message failure:

1. Using the Windows Registry Editor, open the following registry entry on the server: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

2. Edit the entry as follows:

WARNING! **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

- `ResendMailbox` <Administrator Mailbox> (for example, admin@example.com)
- `ResendMailboxDomain` <Administrator's Domain> (for example, example.com)
- `ResendMailSender` <Administrator's Email Account> (for example, admin

3. Close the Registry Editor.

MSA SQL Server Dependency in Exchange Server 2007

In computers running Exchange Server 2007, the Messaging Security Agent (MSA) uses a SQL Server database. To prevent issues, MSA services are designed to be dependent on the SQL Server service instance **MSSQL$SCANMAIL**. Whenever this instance is stopped or restarted, the following MSA services are also stopped:

- ScanMail_Master
- ScanMail_RemoteConfig

Manually restart these MSA services if **MSSQL$SCANMAIL** is stopped or restarted. Different events, including when SQL Server is updated, can cause **MSSQL$SCANMAIL** to restart or stop.

Saving and Restoring Program Settings

You can save a copy of the WFBS-A database and important configuration files for rolling back your WFBS-A program. You may want to do this if you are experiencing problems and want to reinstall WFBS-A or if you want to revert to a previous configuration.

To restore program settings after rollback or reinstallation:

1. Stop the Trend Micro Security Server Master Service.
2. Manually copy the following files and folders from the folder to an alternate location:

   WARNING! Do not use backup tools or applications for this task.

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

   - **`ofcscan.ini`:** Contains global settings.
   - **`ous.ini`:** Contains the update source table for antivirus component deployment.
   - **`Private` folder:** Contains firewall and update source settings.
   - **`Web\TmOPP` folder:** Contains Outbreak Defense settings.
   - **`Pccnt\Common\OfcPfw.dat`:** Contains firewall settings.
   - **`Download\OfcPfw.dat`:** Contains firewall deployment settings.
   - **`Log` folder:** Contains system events and the verify connection log.
   - **`Virus` folder:** The folder in which WFBS-A quarantines infected files.
   - **`HTTDB` folder:** Contains the WFBS-A database.
3. Uninstall WFBS-A.
4. Perform a fresh install. Refer to the WFBS-A *Installation Guide*.
5. After the master installer finishes, stop the Trend Micro Security Server Master Service on the target computer.
6. Update the virus pattern version from the backup file:
   a. Get current virus pattern version from the new server.

   ```
   \Trend Micro\Security Server\PCCSRV\Private\component.ini.
   [6101]

   ComponentName=Virus pattern

   Version=xxxxxx 0 0
   ```

b. Update the version of the virus pattern in the backed-up file:

`\Private\component.ini`

Note: If you change the Security Server installation path, you will have to update the path info in the backup files `ofcscan.ini` and `\private\ofcserver.ini`

---

7. With the backups you created, overwrite the WFBS-A database and the relevant files and folders on the target machine in the `PCCSRV` folder.
8. Restart the Trend Micro Security Server Master Service.

Some Components are not Installed

Licenses to various components of Trend Micro products may differ by region. After installation, you will see a summary of the components your Registration Key/Activation Code allows you to use. Check with your vendor or reseller to verify the components for which you have licenses.

Unable to Access the Web Console

This section discusses the possible causes for being unable to access the Web console.

Browser Cache

If you upgraded from a previous version of WFBS-A, Web browser and proxy server cache files may prevent the Web console from loading. Clear the cache memory on your browser and on any proxy servers located between the Trend Micro Security Server and the computer you use to access the Web console.

SSL Certificate

Also, verify that your Web server is functioning properly. If you are using SSL, verify that the SSL certificate is still valid. See your Web server documentation for details.

Virtual Directory Settings

There may be a problem with the virtual directory settings if you are running the Web console on an IIS server and the following message appears:

The page cannot be displayed
HTTP Error 403.1 - Forbidden: Execute access is denied.
Internet Information Services (IIS)

This message may appear when either of the following addresses is used to access the console:

```
http://<server name>/SMB/
```

```
http://<server name>/SMB/default.htm
```

However, the console may open without any problems when using the following address:

```
http://<server name>/SMB/console/html/cgi/cgichkmasterpwd.exe
```

To resolve this issue, check the execute permissions of the SMB virtual directory.

To enable scripts:

1. Open the Internet Information Services (IIS) manager.
2. In the SMB virtual directory, select **Properties**.
3. Select the **Virtual Directory** tab and change the execute permissions to **Scripts** instead of none. Also, change the execute permissions of the client install virtual directory.

Incorrect Number of Clients on the Web Console

You may see that the number of clients reflected on the Web console is incorrect.

This happens if you retain client records in the database after removing the agent. For example, if client-server communication is lost while removing the agent, the server does not receive notification about the agent removal. The server retains client information in the database and still shows the client icon on the console. When you reinstall the agent, the server creates a new record in the database and displays a new icon on the console.

Use the Verify Connection feature through the Web console to check for duplicate client records.

Client Icon Does Not Appear After Installation

You may discover that the client icon does not appear on the Web console after you install the agent. This happens when the client is unable to send its status to the server.

To check communication between Clients and the Web console:

- Open a Web browser on the client, type `https://{Trend Micro Security Server_Name}:{port number}/SMB/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows "-2", this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record of the client.
- Verify that client-server communication exists by using ping and telnet.
- If you have limited bandwidth, check if it causes connection timeout between the server and the client.
- Check if the \PCCSRV folder on the server has shared privileges and if all users have been granted full control privileges.
- Verify that the Trend Micro Security Server proxy settings are correct.

Issues During Migration from Other Antivirus Software

This section discusses some issues you may encounter when migrating from third-party antivirus software.

The setup program for the Client/Server Security Agent uses the third-party software's uninstallation program to automatically remove it from your users' system and replace it with the Client/Server Security Agent. If automatic uninstallation is unsuccessful, users get the following message:

```
Uninstallation failed.
```

There are several possible causes for this error:

- The third-party software's version number or product key is inconsistent.
- The third-party software's uninstallation program is not working.
- Certain files for the third-party software are either missing or corrupted.
- The registry key for the third-party software cannot be cleaned.
- The third-party software has no uninstallation program.

There are also several possible solutions for this error:

- Manually remove the third-party software.
- Stop the service for the third-party software.
- Unload the service or process for the third-party software.

Unsuccessful Web Page or Remote Installation

If users report that they cannot install from the internal Web page or if installation with Remote install is unsuccessful, try the following methods.

- Verify that client-server communication exists by using ping and telnet.
- Check if TCP/IP on the client is enabled and properly configured.
- If you are using a proxy server for client-server communication, check of the proxy settings are configured correctly.
- In the Web browser, delete Trend Micro add-ons and the browsing history.

Unable to Replicate Messaging Security Agent Settings

You can only replicate settings from a source Messaging Security Agent to a target Messaging Security Agent that share the same domain.

For Windows 2003, do the first 4 steps:

1. Start **regedit**.
2. Go to

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
   ```

3. Right click **winreg > Permissions**.
4. Add **Smex Admin Group** of target domain, and enable **Allow Read**.

   For Windows 2000, also do the following:

5. Go to

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

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

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

Frequently Asked Questions (FAQs)

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

Where Can I Find My Activation Code and Registration Key?

You can activate WFBS-A during the installation process or later using the Web console. To activate WFBS-A, you need to have an Activation Code.

Obtaining an Activation Code

You automatically get an evaluation Activation Code if you download Worry-Free Business Security from the Trend Micro Web site.

You can use a Registration Key to obtain an Activation Code online.

Activation Codes have 37 characters and look like this:

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

Obtaining a Registration Key

The Registration Key can be found on:

- Product CD
- License Certificate (which you obtained after purchasing the product)

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

- Updates to the WFBS-A pattern files and scan engine
- Technical support
- Easy access in viewing the license expiration update, registration and license information, and renewal reminders
- Easy access in renewing your license and updating the customers profile

Registration Keys have 22 characters and look like this:

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

When the full version expires, security updates will be disabled; when the evaluation period expires, both the security updates and scanning capabilities will be disabled. In the Product License screen, you can obtain an Activation Code online, view renewal instructions, and check the status of your product.

Registration

I have several questions on registering WFBS-A. Where can I find the answers?

See the following Web site for frequently asked questions about registration:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Installation, Upgrade, and Compatibility

Which versions of Worry-Free Business Security or Worry-Free Business Security Advanced can upgrade to this version?

Refer to the WFBS-A *Installation Guide* for information.

Which Agent installation method is best for my network environment?

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

Can the Trend Micro Security Server be installed remotely using Citrix or Windows Terminal Services?

Yes. The Trend Micro Security Server can be installed remotely with Citrix or Windows Terminal Services.

Does WFBS-A support 64-bit platforms?

Yes. A scaled down version of the Client/Server Security Agent is available for the x64 platform. However, no support is currently available for the IA-64 platform.

Can I upgrade to WFBS-A from Trend Micro™ ServerProtect?

No. ServerProtect will have to be first uninstalled and then WFBS-A can be installed.

Can I use a pre-existing installation of an Apache Web server on computer where I am installing the Security Server?

Trend Micro recommends that you do not use a pre-existing installation of Apache. The correct version will be installed at the same time that you install the Security Server.

How Can I Recover a Lost or Forgotten Password?

Access to the Worry-Free Business Security console requires a password, which is first defined during installation and can be subsequently changed at any time. Contact Support if you lost or forgot your password.

Intuit Software Protection

What happens when an attempted Intuit update is blocked?

All Intuit executable files have a digital signature and updates to these files will not be blocked. If there are other programs try to change the Intuit binary file, the agent displays a message with the name of the program that is attempting to update the binary files.

Can other programs be allowed to update Intuit files? Can I bypass Trend Micro protection on a case-to-case basis?

Yes. To allow this, add the required program to the Behavior Monitoring Exception List on the agent.

WARNING! **Remember to remove the program from the exception list after the update.**

Configuring Settings

I have several questions on configuring WFBS-A settings. Where can I find the answers?

You can download all WFBS-A documentation from the following site:

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

What folders should I exclude for Antivirus software with SBS 2003?

Refer to the following tables for the SBS 2003 exclusions:

TABLE F-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 F-2. IIS Exclusions

IIS System Files	C:\WINDOWS\system32\inetsrv
IIS Compression Folder	C:\WINDOWS\IIS Temporary Compressed Files

TABLE F-3. Domain Controller Exclusions

Active Directory database files	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
NTFRS Database Files	C:\WINDOWS\ntfrs

TABLE F-4. Windows SharePoint Services Exclusions

Temporary SharePoint folder	C:\windows\temp\FrontPageTempDir

TABLE F-5. Client Desktop Folder Exclusions

Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore

TABLE F-6. Additional Exclusions

Removable Storage Database (used by SBS Backup)	C:\Windows\system32\NtmsData
SBS POP3 connector Failed Mail	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail
SBS POP3 connector Incoming Mail	C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail
Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore
DHCP Database Store	C:\WINDOWS\system32\dhcp
WINS Database Store	C:\WINDOWS\system32\wins

Do I Have the Latest Pattern File or Service Pack?

The updatable files will very depending on which product you have installed.

To find out if you have the latest pattern file or service pack:

1. From the Web console, click **Preferences > Product License**. The Product License screen appears.
2. Product license details, including the current product version appears.

To find out the latest available patterns, open a Web browser to one of the following:

- The Trend Micro Update Center:

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

- The Trend Micro Pattern File:

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

Smart Scan

What is Smart Scan?

Smart Scan is a new technology from Trend Micro that uses a central scan server on the network to take some of the burden of scanning off clients.

Is Smart Scan reliable?

Yes. Smart Scan simply allows another computer, the Smart Scan Server, to help scan your clients. If your clients are configured for Smart Scan but cannot connect to the Smart Scan Server, they will attempt to connect to the Trend Micro Global Smart Scan Server.

How do I know if the Smart Scan Server is running properly?

Verify that the following service is running on the Security Server:

```
TMiCRCScanService
```

Can I uninstall the Scan Server or choose not to install it?

No. Use Conventional Scan if you do not want to use Smart Scan.

Also see *Scan Methods* on page 8-2.

Known Issues

Known issues are features in WFBS-A software that may temporarily require a workaround. Known issues are typically documented in the Readme document you received with your product. Readme files for Trend Micro products can also be found in the Trend Micro Update Center:

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

Known issues can be found in the technical support Knowledge Base:

http://esupport.trendmicro.com/support/

Trend Micro recommends that you always check the Readme text for information on known issues that could affect installation or performance, as well as a description of what is new in a particular release, system requirements, and other tips.

Appendix G

Getting Help

This appendix shows you how to get help, find additional information, and contact Trend Micro.

The topics discussed in this appendix include:

Product Documentation

The documentation for WFBS-A consists of the following:

- Online Help

  Web-based documentation accessible from the Web console.

  The WFBS-A *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.

- Installation Guide

  The *Installation Guide* provides instructions to install/upgrade the product and get started. It provides a description of the basic features and default settings of WFBS-A.

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

  http://www.trendmicro.com/download

  Who should read this guide?

  WFBS-A Administrators who want to install and get started with WFBS-A.

- 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 WFBS-A.

- Readme file

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

- Knowledge Base

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

  http://esupport.trendmicro.com

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

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

Knowledge Base

The Trend Micro Knowledge Base is an online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use the Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in the Knowledge Base are product FAQs, tips, advice on preventing virus/malware infections, and regional contact information for support and sales.

The Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

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

Technical Support

When you contact Trend Micro Technical Support, to speed up your problem resolution, run the Case Diagnostic Tool (refer *Using the Case Diagnostic Tool* on page G-4) or ensure that you have the following details available:

- Operating system
- Network type
- Brand and model of the computer and connected hardware
- Amount of memory and free hard disk space on your machine

- Detailed description of the installation environment
- Exact text of any error message
- Steps to reproduce the problem

To contact Trend Micro Technical Support:

1. Run the Case Diagnostic Tool. For more information, refer *Using the Case Diagnostic Tool* on page G-4.
   - Visit the following URL:

     http://esupport.trendmicro.com/support/srf/questionentry.do

     Click the link for the required region. Follow the instructions for contacting support in your region.
   - If you prefer to communicate by email message, send a query to the following address:

     virusresponse@trendmicro.com
   - In the United States, you can also call the following toll-free telephone number:

     `(877) TRENDAV, or 877-873-6328`

Using the Case Diagnostic Tool

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

Download the Case Diagnostic Tool from:

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

Contacting Trend Micro

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

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

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

Sending Suspicious Files to Trend Micro

You can send your virus/malware, infected files, Trojans, suspected worms, and other suspicious files to Trend Micro for evaluation. To do so, contact your support provider or visit the Trend Micro Submission Wizard URL:

http://subwiz.trendmicro.com/SubWiz

Click the link under the type of submission you want to make.

Note: Submissions made through the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you submit your case, an acknowledgement screen displays. This screen also displays a case number. Make note of the case number for tracking purposes.

Trend Micro Virus Information Center

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

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

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of threats expected to trigger in the current week and describes the 10 most prevalent threats around the globe for the current week.
- View a Virus Map of the top 10 threats around the globe.
- Consult the Virus Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes.
- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured.

- Read general virus/malware information, such as:
  - The Virus Primer, which helps you understand the difference between virus/malware, Trojans, worms, and other threats
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
  - A glossary of virus/malware and other security threat terminology
- Download comprehensive industry white papers
- Subscribe to Trend Micro Virus Alert service to learn about outbreaks as they happen and the Weekly Virus Report
- Learn about free virus/malware update tools available to Web masters. Read about TrendLabs^{SM}, the Trend Micro global antivirus research and support center

About TrendLabs

TrendLabs is the Trend Micro global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Lake Forest, CA, to mitigate virus outbreaks and provide urgent support 24x7.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

Appendix H

Glossary

The Glossary provides descriptions of important terms and concepts used in this document. For information on security threats, see:
http://threatinfo.trendmicro.com/vinfo/

For information about how the Trend Micro Smart Protection Network protects you, see:
http://itw.trendmicro.com/smart-protection-network

Term	Description
Activation Code	A numerical code required to enable scanning and product updates. You can activate your product during installation or anytime thereafter. If you do not have the Activation Code(s), use the Registration Key that came with your product to register on the Trend Micro Web site and receive the Activation Code(s).
ActiveUpdate	Connected to the Trend Micro update Web site, ActiveUpdate provides updated downloads of components such as the virus pattern files, scan engines, and program files. ActiveUpdate is a function common to many Trend Micro products.
Administrator	A type of virus that resides in Web pages that execute ActiveX controls.
Agent	The WFBS-A program that runs on the client.
clean	To remove virus code from a file or message.
Cleanup	Cleanup detects and removes Trojans and applications or processes installed by Trojans. It repairs files modified by Trojans.
Clients	Clients are Microsoft Exchange servers, desktops, portable computers, and servers where a Messaging Security Agent or a Client/Server Security Agent is installed.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
Content Filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
Conventional Scan	A local scan engine on the client scans the client computer.

Term	Description
End User License Agreement (EULA)	An End User License Agreement, or EULA, is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking “I accept” during installation. Clicking “I do not accept” will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware/grayware and other types of grayware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software.
Live Status	The main screen or dashboard of the Web Console. Live Status gives you an at-a-glance security status for Outbreak Defense, Antivirus, Anti-spyware, and Network Viruses.
pattern matching	Since each virus contains a unique “signature” or string of telltale characters that distinguish it from any other code, the virus experts at Trend Micro capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When the engine detects a match, a virus has been detected and an email notification is sent to the Administrator.
privileges (client privileges)	From the Web console, Administrators can set privileges for the Client/Server Security Agents. End users can then set the Client/Server Security Agents to scan their clients according to the privileges you allowed. Use client privileges to enforce a uniform antivirus policy throughout your organization.
Registration Key	A numerical code required to register with Trend Micro and obtain an Activation Code.
Scan Server	A server that helps scan clients so clients do not have to complete the whole scanning process themselves.

Term	Description
Security Server	When you first install WFBS-A, you install it on a Windows server that becomes the Security Server. The Security Server communicates with the Client/Server Security Agents and the Messaging Security Agents installed on clients. The Security Server also hosts the Web console, the centralized Web-based management console for the entire WFBS-A solution.
Smart Scan	A Scan Server helps scan the client.
TrendLabs	TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.
TrendSecure	TrendSecure comprises a set of browser-based plugin tools (TrendProtect and Transaction Protector) that enable users to surf the Web securely. TrendProtect warns users about malicious and Phishing Web sites. Transaction Protector determines the safety of your wireless connection by checking the authenticity of the access point.
Update Agent	Agents that act as update sources for other agents.
Web console	The Web console is a centralized Web-based management console. You can use it to configure the settings of Client/Server Security Agents and Messaging Security Agents which are protecting all your remote desktops, servers and Microsoft Exchange servers. The Web console is installed when you install the Trend Micro Security Server and uses Internet technologies such as ActiveX, CGI, HTML, and HTTP.

Index

A

B

C

G

H

I

O

P

Q

T

U

V

W

Y