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


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

Copyright © 2012 Trend Micro Incorporated. All rights reserved.

Document Part No.: WFEM85491/120709

Release Date: December 2012

Protected by U.S. Patent No. 5,951,698 and 7,188,369

The user documentation for Trend Micro Worry-Free Business Security introduces the main features of the software and installation instructions for your production environment. Read through it before 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 online Knowledge Base at Trend Micro’s website.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp
# Table of Contents

## Preface

Preface ................................................................................................................................. xi
Worry-Free Business Security Documentation ................................................................ xii
Audience ............................................................................................................................. xii
Document Conventions ..................................................................................................... xiii

## Chapter 1: Introducing Worry-Free Business Security

**Standard and Advanced**

Overview of Trend Micro Worry-Free Business Security ................................. 1-2
New in this Release ........................................................................................................... 1-2
Key Features and Benefits ............................................................................................. 1-3
  Trend Micro Smart Protection Network ................................................................. 1-3
  File Reputation Services .......................................................................................... 1-4
  Web Reputation Services ....................................................................................... 1-4
  Email Reputation (Advanced only) ................................................................. 1-5
  Smart Feedback ................................................................................................. 1-5
  URL Filtering ...................................................................................................... 1-6
Benefits of Protection ..................................................................................................... 1-7
Understanding Threats ................................................................................................. 1-8
  Viruses and Malware ............................................................................................ 1-8
  Spyware and Grayware ......................................................................................... 1-10
  Spam ..................................................................................................................... 1-11
  Intrusions ............................................................................................................... 1-11
  Malicious Behavior ............................................................................................. 1-11
  Fake Access Points ............................................................................................. 1-11
Explicit/Restricted Content in Instant Messaging (IM) Applications ................. 1-11
Phishing Incidents ........................................................................................................ 1-12
Mass Mailing Attacks ................................................................................................. 1-12
Web Threats ................................................................................................................. 1-13
Chapter 2: Getting Started

The Worry-Free Business Security Network ................................................. 2-2
Security Server ........................................................................................................ 2-2
Scan Server ........................................................................................................ 2-2
Agents ..................................................................................................................... 2-3
Web Console ........................................................................................................... 2-4
  Opening the Web Console ................................................................................ 2-5
  Web Console Navigation .................................................................................... 2-7
  Web Console Icons .................................................................................................. 2-10
  Live Status .............................................................................................................. 2-11

Chapter 3: Installing Agents

Security Agent Installation .................................................................................... 3-2
  Security Agent Installation Requirements ......................................................... 3-2
  Security Agent Installation Considerations ........................................................ 3-2
  Available Security Agent Features ...................................................................... 3-3
  Security Agent Installation and IPv6 Support ...................................................... 3-6
Security Agent Installation Methods ..................................................................... 3-8
  Installing from the Internal Web Page ................................................................. 3-10
  Installing with Login Script Setup ....................................................................... 3-13
  Installing with Client Packager ............................................................................ 3-14
  Installing with Remote Install ............................................................................... 3-18
  Installing with Vulnerability Scanner ................................................................. 3-21
  Installing with Email Notification ........................................................................ 3-31
  Migrating to the Security Agent .......................................................................... 3-32
  Performing Post-installation Tasks on Security Agents ........................................ 3-33
Messaging Security Agent Installation ................................................................. 3-35
  Messaging Security Agent Installation Requirements ......................................... 3-35
  Installing the Messaging Security Agent (Advanced only) ................................... 3-35
Removing Agents .................................................................................................. 3-37
  Removing Agents from the Web Console ............................................................... 3-38
  Uninstalling Agents from the Web Console ............................................................ 3-39
  Uninstalling the Security Agent from the Client ...................................................... 3-40
  Using the SA Uninstall Tool .................................................................................. 3-40
Uninstalling the Messaging Security Agent from the Microsoft Exchange Server (Advanced Only) ................................................... 3-42

Chapter 4: Managing Groups

Groups .............................................................................................................. 4-2
Adding Groups ............................................................................................. 4-10
Adding Agents to Groups ........................................................................... 4-11
Moving Agents .............................................................................................. 4-12
   Moving Security Agents Between Groups ................................................. 4-13
   Moving Agents Between Security Servers Using the Web Console .................................................................................................................. 4-14
   Moving a Security Agent Between Security Servers Using Client Mover ......................................................................................................... 4-15
Replicating Settings ...................................................................................... 4-17
   Replicating Security Agent Group Settings .............................................. 4-17
   Replicating Messaging Security Agent Settings (Advanced only) . 4-18
Importing and Exporting the Settings of Security Agent Groups ...... 4-19
   Exporting Settings ................................................................................ 4-21
   Importing Settings ................................................................................ 4-22

Chapter 5: Managing Basic Security Settings for Security Agents

Summary of Basic Security Settings for Security Agents ....................... 5-2
Scan Methods ............................................................................................... 5-3
   Configuring Scan Methods ................................................................... 5-5
Real-time Scan for Security Agents .............................................................. 5-7
   Configuring Real-time Scan for Security Agents ................................. 5-7
Firewall .......................................................................................................... 5-8
   Configuring the Firewall ....................................................................... 5-10
   Working with Firewall Exceptions ...................................................... 5-12
Disabling the Firewall on a Group of Agents ......................................... 5-14
Disabling the Firewall on All Agents ..................................................... 5-14
Chapter 6: Managing Basic Security Settings for Messaging Security Agents (Advanced Only)

Messaging Security Agents ................................................................. 6-2
   How the Messaging Security Agent Scans Email Messages .......... 6-3
   Default Messaging Security Agent Settings ............................. 6-3

Real-Time Scan for Messaging Security Agents ................................. 6-5
   Configuring Real-time Scan for Messaging Security Agents ........ 6-5
Anti-Spam ........................................................................................... 6-6
   Email Reputation .............................................................. 6-7
   Content Scanning ............................................................. 6-8

Content Filtering ................................................................................... 6-14
   Managing Content Filtering Rules ........................................... 6-15
   Types of Content Filtering Rules .......................................... 6-18
   Adding a Content Filtering Rule for All Matching Conditions .... 6-19
   Adding a Content Filtering Rule for Any Matching Condition .... 6-22
   Adding a Content Filtering Monitoring Rule ......................... 6-24
<table>
<thead>
<tr>
<th>Chapter 7: Managing Scans</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Scans .................. 7-2</td>
</tr>
<tr>
<td>Real-time Scan ................. 7-2</td>
</tr>
<tr>
<td>Manual Scan .................... 7-3</td>
</tr>
<tr>
<td>Running Manual Scans .......... 7-3</td>
</tr>
<tr>
<td>Scheduled Scan ................ 7-6</td>
</tr>
<tr>
<td>Configuring Scheduled Scans .... 7-6</td>
</tr>
</tbody>
</table>
Chapter 8: Managing Updates

Update Overview ................................................................. 8-2
Updatable Components .......................................................... 8-3
  Hot Fixes, Patches, and Service Packs .................................. 8-9
Security Server Updates .......................................................... 8-9
  Configuring the Security Server Update Source ...................... 8-11
  Updating the Security Server Manually .................................. 8-12
  Configuring Scheduled Updates for the Security Server ........... 8-13
  Rolling Back Components .................................................. 8-14
Security Agent and Messaging Security Agent Updates ............... 8-14
Update Agents ........................................................................ 8-16
  Configuring Update Agents .................................................. 8-18

Chapter 9: Managing Notifications

Notifications ........................................................................ 9-2
  Configuring Events for Notifications ..................................... 9-3
    Token Variables .................................................................. 9-4

Chapter 10: Using Outbreak Defense

Outbreak Defense Strategy .................................................... 10-2
Vulnerability Assessment ....................................................... 10-4
Outbreak Prevention Policy .................................................... 10-5
Outbreak Defense Current Status .......................................... 10-6
  Automatic Outbreak Defense Details .................................... 10-8
Outbreak Defense Potential Threat ........................................ 10-8
  Vulnerability Assessment Pattern File .................................. 10-10
  Damage Cleanup Services .................................................. 10-10
Configuring Outbreak Defense Settings .................................. 10-11
  Outbreak Defense Exceptions ............................................. 10-14
Chapter 11: Managing Global Settings

- Global Settings ............................................................... 11-2
- Configuring Internet Proxy Settings .............................. 11-3
- Configuring SMTP Server Settings ............................... 11-4
- Configuring Desktop/Server Settings ......................... 11-5
- Configuring System Settings ........................................ 11-11

Chapter 12: Using Logs and Reports

- Logs ......................................................................................... 12-2
  - Using Log Query .............................................................. 12-4
- Reports ..................................................................................... 12-5
  - Working with One-time Reports .................................. 12-5
  - Working with Scheduled Reports .............................. 12-7
  - Interpreting Reports ......................................................... 12-11
- Performing Maintenance Tasks for Reports and Logs .... 12-14

Chapter 13: Performing Administrative Tasks

- Changing the Web Console Password .......................... 13-2
- Working with Plug-in Manager ................................. 13-2
- Managing the Product License ............................... 13-3
- Participating in the Smart Feedback Program ............. 13-5
- Changing the Agent’s Interface Language .................. 13-5
- Saving and Restoring Program Settings ..................... 13-5
- Uninstalling the Security Server ................................. 13-8

Chapter 14: Using Management Tools

- Tool Types .............................................................................. 14-2
- Installing the Trend Micro Worry-Free Remote Manager Agent 14-3
Saving Disk Space ................................................................. 14-5
Running Disk Cleaner on the Security Server .................. 14-6
Running Disk Cleaner on the Security Server Using the Command Line Interface ......................................................... 14-7
Saving Disk Space on Clients .............................................. 14-8

Moving the Scan Server Database ......................................... 14-8
Restoring Encrypted Files ....................................................... 14-9
Decrypting and Restoring Files on the Security Agent .......... 14-10
Decrypting and Restoring Files on the Security Server, Custom Quarantine Directory, or Messaging Security Agent .......... 14-11
Restoring Transport Neutral Encapsulation Format Email Messages ....................................................................................... 14-13

Using the ReGenID Tool ......................................................... 14-13
Managing SBS and EBS Add-ins .............................................. 14-14
Installing the SBS and EBS Add-ins Manually ....................... 14-14
Using the SBS or EBS Add-ins .............................................. 14-15

Appendix A: Security Agent Icons
Checking the Security Agent Status ........................................ A-2
Viewing Security Agent Icons on the Windows Task Bar .......... A-4
Accessing the Console Flyover .............................................. A-4

Appendix B: IPv6 Support in Worry-Free Business Security
Security Server IPv6 Requirements ....................................... B-2
Security Agent Requirements ............................................. B-3
Messaging Security Agent Requirements ................................ B-3
Pure IPv6 Server Limitations ............................................. B-3
Pure IPv6 Agent Limitations ............................................. B-4
Configuring IPv6 Addresses ............................................... B-5
Screens That Display IP Addresses ..................................... B-6

Appendix C: Getting Help
The Trend Micro Knowledge Base ............................................................. C-2
Contacting Technical Support ..................................................................... C-2
    Case Diagnostic Tool ............................................................................ C-3
    Speeding Up Your Support Call .......................................................... C-3
Contact Information ........................................................................................ C-3
Sending Suspicious Files to Trend Micro ................................................... C-4
Security Information Center ........................................................................ C-4
TrendLabs ....................................................................................................... C-5
Documentation Feedback ............................................................................ C-5

**Appendix D: Product Terminology and Concepts**

- Hot Fix ............................................................................................................ D-2
- IntelliScan ....................................................................................................... D-2
- IntelliTrap ....................................................................................................... D-2
- Intrusion Detection System ......................................................................... D-4
- Keywords ........................................................................................................ D-5
- Patch ................................................................................................................ D-9
- Regular Expressions ...................................................................................... D-9
- Scan Exclusion Lists ..................................................................................... D-18
- Security Patch .............................................................................................. D-25
- Service Pack ................................................................................................. D-25
- Trojan Port ..................................................................................................... D-25
- Uncleanable Files ........................................................................................ D-26

**Index**

Index .............................................................................................................. IN-1
Preface

Worry-Free Business Security Documentation

Worry-Free Business Security documentation includes the following:

**TABLE 1. Worry-Free Business Security Documentation**

<table>
<thead>
<tr>
<th>DOCUMENTATION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation and Upgrade Guide</td>
<td>A PDF document that discusses requirements and procedures for installing the Security Server, and upgrading the server and agents</td>
</tr>
<tr>
<td>Administrator's Guide</td>
<td>A PDF document that discusses getting started information, client installation procedures, and Security Server and agent management</td>
</tr>
<tr>
<td>Help</td>
<td>HTML files compiled in WebHelp or CHM format that provide &quot;how to's&quot;, usage advice, and field-specific information</td>
</tr>
<tr>
<td>Readme file</td>
<td>Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: <a href="http://esupport.trendmicro.com/en-us/business/default.aspx">http://esupport.trendmicro.com/en-us/business/default.aspx</a></td>
</tr>
</tbody>
</table>

Download the latest version of the PDF documents and readme at:


**Audience**

Worry-Free Business Security documentation is intended for the following users:

- **Security Administrators**: Responsible for Worry-Free Business Security management, including Security Server and agent installation and management. These users are expected to have advanced networking and server management knowledge.
• **End users**: Users who have the Security Agent installed on their computers. The computer skill level of these individuals ranges from beginner to power user.

### Document Conventions

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

**Table 2. Document Conventions**

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ALL CAPITALS</strong></td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, options, and tasks</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>References to other documentation or new technology components</td>
</tr>
<tr>
<td><code>&lt;Text&gt;</code></td>
<td>Indicates that the text inside the angle brackets should be replaced by actual data. For example, C:\Program Files &lt;file_name&gt; can be C:\Program Files\sample.jpg</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Provides configuration notes or recommendations</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>Provides best practice information and Trend Micro recommendations</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td>Provides warnings about activities that may harm computers on your network</td>
</tr>
</tbody>
</table>
Chapter 1

Introducing Worry-Free™ Business Security Standard and Advanced

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

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

This document provides information for both WFBS Standard and Advanced. Sections and chapters relevant to the Advanced version only are marked as “(Advanced only)”.

Powered by the Trend Micro Smart Protection Network, WFBS is:

- **Safer**: Stops viruses, spyware, spam (Advanced only), and web threats from reaching clients. URL filtering blocks access to risky websites and helps improve user productivity.

- **Smarter**: Fast scans and continuous updates prevent new threats, with minimal impact to clients.

- **Simpler**: Easy to deploy and requiring zero administration, WFBS detects threats more effectively so that you can focus on business instead of security.

New in this Release

Worry-Free Business Security includes the following new features and enhancements.

- **Platform support**: The Security Server and Security Agents can now be installed on Windows 8 and Windows Server 2012.

- **IPv6 support**: The Security Server, Security Agents, Messaging Security Agents (Advanced only), and Remote Manager Agent can now be installed on IPv6 clients.

- **Advanced cleanup**: When configured to run advanced cleanup, Security Agents can stop activities by rogue security software, also known as FakeAV. The agent also uses advanced cleanup rules to proactively detect and stop applications that exhibit FakeAV behavior.

Enable advanced cleanup on Security Agents when you configure your Manual Scan and Scheduled Scan settings.
• **Action against probable virus/malware**: For probable virus/malware, the default action is "Deny Access" during Real-time Scan and "Pass" during Manual Scan and Scheduled Scan. If these are not your preferred actions, you can change them to Quarantine, Delete, or Rename.

• **Client shutdown after Scheduled Scan**: A new setting in the web console (Scans > Scheduled Scan > Schedule tab) allows agents to initiate a shutdown of the client after completing a Scheduled Scan. This setting can only be configured from the web console and is not available to users with Scheduled Scan privileges.

• **Security Agent installation path**: During the Security Server installation, you are prompted to specify the installation path where Security Agents are installed. In previous versions, the installation path cannot be changed when the Security Server installation has been completed. In this version, you can change the installation path from the web console by navigating to Preferences > Global Settings > System > Security Agent Installation directory section. After changing the path, new Security Agents will be installed to this path.

• **Scan Server Database Mover**: This tool moves the Scan Server database safely to another disk drive. See *Moving the Scan Server Database on page 14-8*.

### Key Features and Benefits

Worry-Free Business Security provides the following features and benefits:

**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 security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. Smart Protection Network uses lighter-weight clients to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. Customers’ protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.
For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

File Reputation Services

File Reputation Services checks the reputation of each file against an extensive in-the-cloud database. 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.

Security Agents must be in smart scan mode to use File Reputation Services. These agents are referred to as smart scan agents in this document. Agents that are not in smart scan mode do not use File Reputation Services and are called conventional scan agents. Worry-Free Business Security administrators can configure all or several agents to be in smart scan mode.

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. Web reputation then continues to scan sites and block users from accessing infected ones. Web reputation features help ensure that the pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. 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.

Agents subject to web reputation policies use Web Reputation Services. Worry-Free Business Security administrators can subject all or several agents to web reputation policies.
Email Reputation (Advanced only)

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

Email Reputation technology identifies spam based on the reputation of the originating Mail Transport Agent (MTA). This off-loads the task from the Security Server. With Email Reputation enabled, all inbound SMTP traffic is checked by the IP databases to see whether the originating IP address is clean or 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.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and its 24/7 threat research centers and technologies. Each new threat identified through every single customer's routine reputation check automatically updates all 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 the protection of others. Because the gathered threat information 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.

Samples of information sent to Trend Micro:

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

You can terminate your participation to the program anytime from the web console. For details, see Participating in the Smart Feedback Program on page 13-5.

---

**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.smartprotectionnetwork.com

---

**URL Filtering**

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

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

**Table 1-1. Benefits of Protection**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virus/Malware.</strong> Virus, Trojans, Worms, Backdoors, and Rootkits</td>
<td>File-based scans (Real-time Scan, Manual Scan, Scheduled Scan)</td>
</tr>
<tr>
<td><strong>Spyware/Grayware.</strong> Spyware, Dialers, Hacking tools, Password cracking applications, Adware, Joke programs, and Keyloggers</td>
<td></td>
</tr>
<tr>
<td>Security threats transmitted through email messages</td>
<td>POP3 Mail Scan in the Security Agent</td>
</tr>
<tr>
<td></td>
<td>IMAP Mail Scan in the Messaging Security Agent</td>
</tr>
<tr>
<td></td>
<td><strong>Anti-spam, Content Filtering, Data Loss Prevention, Attachment Blocking,</strong> and <strong>Web Reputation</strong> in the Messaging Security Agent</td>
</tr>
<tr>
<td>Network worms/viruses and intrusions</td>
<td>Firewall in the Security Agent</td>
</tr>
<tr>
<td>Conceivably harmful websites/Phishing sites</td>
<td>Web Reputation and URL Filtering in the Security Agent</td>
</tr>
<tr>
<td>Security threats that spread through USB and other external devices</td>
<td>Device Control in the Security Agent</td>
</tr>
<tr>
<td>Malicious behavior</td>
<td>Behavior Monitoring in the Security Agent</td>
</tr>
<tr>
<td>Fake access points</td>
<td>Wi-Fi Advisor in the Security Agent</td>
</tr>
<tr>
<td>Explicit/restricted content in IM applications</td>
<td>IM Content Filtering in the Security Agent</td>
</tr>
</tbody>
</table>
Understanding Threats

Organizations without dedicated security personnel and with lenient security policies are increasingly exposed to threats, even if they have basic security infrastructure in place. Once discovered, these threats may have already spread to many computing resources, taking considerable time and effort to eliminate completely. Unforeseen costs related to threat elimination can also be staggering.

Trend Micro network security intelligence and in-the-cloud servers that are part of Trend Micro Smart Protection Network identify and respond to next-generation threats.

Viruses and Malware

Tens of thousands of virus/malware exist, with more being created each day. Although once most common in DOS or Windows, computer viruses today can cause a great amount of damage by exploiting vulnerabilities in corporate networks, email systems and websites.

• **Joke program**: A virus-like program that often manipulates the appearance of things on a computer monitor.

• **Probable virus/malware**: Suspicious files that have some of the characteristics of virus/malware. For details, see the Trend Micro Threat Encyclopedia:

• **Rootkit**: A program (or collection of programs) that installs and executes code on a system without end user consent or knowledge. It uses stealth to maintain a persistent and undetectable presence on the machine. Rootkits do not infect machines, but rather, seek to provide an undetectable environment for malicious code to execute. Rootkits are installed on systems via social engineering, upon execution of malware, or simply by browsing a malicious website. Once installed, an attacker can perform virtually any function on the system to include remote access, eavesdropping, as well as hide processes, files, registry keys and communication channels.

• **Trojan horse**: This type of threat often uses ports to gain access to computers or executable programs. Trojan horse programs do not replicate but instead reside on systems to perform malicious acts, such as opening ports for hackers to enter.
Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those already running on the system.

- **Virus**: A program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes, including:
  - **ActiveX malicious code**: Code that resides on web pages that execute ActiveX™ controls.
  - **Boot sector virus**: A virus that infects the boot sector of a partition or a disk.
  - **COM and EXE file infector**: An executable program with .com or .exe extension.
  - **Java malicious code**: Operating system-independent virus code written or embedded in Java™.
  - **Macro virus**: A virus encoded as an application macro and often included in a document.
  - **Network Virus**: A virus spreading over a network is not, strictly speaking, a network virus. Only some virus/malware types, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of client computers, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional file I/O based scanning methods.

The WFBS firewall works with the Common Firewall Pattern to identify and block network viruses.

- **Packer**: A compressed and/or encrypted Windows or Linux™ executable program, often a Trojan horse program. Compressing executables makes packer more difficult for antivirus products to detect.

- **Test virus**: An inert file that acts like a real virus and is detectable by virus-scanning software. Use test viruses, such as the EICAR test script, to verify that your antivirus installation scans properly.
• **VBScript, JavaScript** or **HTML virus**: A virus that resides on web pages and downloaded through a browser.

• **Worm**: A self-contained program or set of programs able to spread functional copies of itself or its segments to other computer systems, often through email.

• **Others**: Virus/Malware not categorized under any of the other virus/malware types.

**Spyware and Grayware**

Clients are at risk from potential threats other than viruses/malware. Spyware/Grayware refers to applications or files not classified as viruses or Trojans, but can still negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization. Often spyware/grayware performs a variety of undesired and threatening actions such as irritating users with pop-up windows, logging user keystrokes, and exposing computer vulnerabilities to attack.

If you find an application or file that Worry-Free Business Security cannot detect as grayware but you think is a type of grayware, send it to Trend Micro for analysis:


• **Spyware**: Gathers data, such as account user names and passwords, and transmits them to third parties.

• **Adware**: Displays advertisements and gathers data, such as user web surfing preferences, used for targeting advertisements at the user through a web browser.

• **Dialer**: Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem. These are often pay-per-call or international numbers that can result in a significant expense for your organization.

• **Joke program**: Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes.

• **Hacking tool**: Helps hackers enter computers.

• **Remote access tool**: Helps hackers remotely access and control computers.
Introducing Worry-Free Business Security Standard and Advanced

- **Password cracking application**: Helps hackers decipher account user names and passwords.
- **Others**: Other types of potentially malicious programs.

**Spam**

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

**Intrusions**

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

**Malicious Behavior**

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

**Fake Access Points**

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

**Explicit/Restricted Content in Instant Messaging (IM) Applications**

Text content that is either explicit or restricted to your organization, such as confidential company information, can pose a threat if transmitted over instant messaging applications.
Phishing Incidents

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

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

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

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

Please report to Trend Micro any website you suspect to be a phishing site. See Sending Suspicious Files to Trend Micro on page C-4 for more information.

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

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.

You can enable the Messaging Security Agent (Advanced only) to take a special action against mass-mailing attacks whenever it detects a mass-mailing behavior. The action set for mass-mailing behavior takes precedence over all other actions. The default action against mass-mailing attacks is delete entire message.
For example: You configure the Messaging Security Agent to quarantine messages when it detects that the messages are infected by a worm or a Trojan. You also enable mass-mailing behavior and set the agent to delete all messages that demonstrate mass-mailing behavior. The agent receives a message containing a worm such as a variant of MyDoom. This worm uses its own SMTP engine to send itself to email addresses that it collects from the infected computer. When the agent detects the MyDoom worm and recognizes its mass-mailing behavior, it will delete the email message containing the worm - as opposed to the quarantine action for worms that do not show mass-mailing behavior.

Web Threats

Web threats encompass a broad array of threats that originate from the Internet. Web threats are sophisticated in their methods, using a combination of various files and techniques rather than a single file or approach. For example, web threat creators constantly change the version or variant used. Because the web threat is in a fixed location of a website rather than on an infected computer, the web threat creator constantly modifies its code to avoid detection.

In recent years, individuals once characterized as hackers, virus writers, spammers, and spyware makers are now known as cyber criminals. Web threats help these individuals pursue one of two goals. One goal is to steal information for subsequent sale. The resulting impact is leakage of confidential information in the form of identity loss. The infected computer may also become a vector to deliver phish attacks or other information capturing activities. Among other impacts, this threat has the potential to erode confidence in web commerce, corrupting the trust needed for Internet transactions. The second goal is to hijack a user’s CPU power to use it as an instrument to conduct profitable activities. Activities include sending spam or conducting extortion in the form of distributed denial-of-service attacks or pay-per-click activities.
Chapter 2

Getting Started

This chapter discusses how to get Worry-Free Business Security up and running.
The Worry-Free Business Security Network

Worry-Free Business Security is comprised of the following:

- **Security Server on page 2-2**
- **Agents on page 2-3**
- **Web Console on page 2-4**

Security Server

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

The Security Server performs these important functions:

- Installs, monitors, and manages agents.
- Downloads the components needed by agents. By default, the Security Server downloads components from the Trend Micro ActiveUpdate server and then distributes them to agents.

Scan Server

The Security Server includes a service called Scan Server, which is automatically installed during Security Server installation. As such, there is no need to install it separately. The Scan Server runs under the process name \icRCService.exe and appears as **Trend Micro Smart Scan Service** from Microsoft Management Console.

When Security Agents use a scan method called **smart scan**, the Scan Server helps these agents run scans more efficiently. The smart scan process can be described as follows:
The Security Agent scans the client for security threats using the **Smart Scan Agent Pattern**, a lightweight version of the traditional Virus Pattern. The Smart Scan Agent Pattern holds most of the threat signatures available on the Virus Pattern.

A Security Agent that cannot determine the risk of the file during the scan verifies the risk by sending a scan query to the Scan Server. The Scan Server verifies the risk using the **Smart Scan Pattern**, which holds the threat signatures not available on the Smart Scan Agent Pattern.

The Security Agent "caches" the scan query result provided by the Scan Server to improve the scan performance.

By hosting some of the threat definitions, the Scan Server helps reduce the Security Agents’ bandwidth consumption when downloading components. Instead of downloading the Virus Pattern, Security Agents download the Smart Scan Agent Pattern, which is significantly smaller in size.

When Security Agents are unable to connect to the Scan Server, they send scan queries to the Trend Micro Smart Protection Network, which has the same function as the Scan Server.

It is not possible to uninstall the Scan Server separately from the Security Server. If you do not want to use the Scan Server:

1. On the Security Server computer, open Microsoft Management Console and disable the **Trend Micro Smart Scan Service**.

2. On the web console, switch Security Agents to conventional scan by navigating to **Preferences > Global Settings > Desktop/Server** tab and selecting the option **Disable Smart Scan Service**.

**Agents**

Agents protect clients from security threats. Clients include desktops, servers, and Microsoft Exchange servers. The WFBS agents are:
TABLE 2-1. WFBS Agents

<table>
<thead>
<tr>
<th>AGENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Agent</td>
<td>Protects desktops and servers from security threats and intrusions</td>
</tr>
<tr>
<td>Messaging Security Agent (Advanced only)</td>
<td>Protects Microsoft Exchange servers from email-borne security threats</td>
</tr>
</tbody>
</table>

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

Web Console

The web console is the central point for monitoring clients throughout the corporate network. It comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console uses standard Internet technologies, such as Java, CGI, HTML, and HTTP.

Use the web console to:

- Deploy agents to clients.
- Organize agents into logical groups for simultaneous configuration and management.
- Set antivirus and anti-spyware scan configurations and start Manual Scan on a single group or on multiple groups.
- Receive notifications and view log reports for threat-related activities.
- Receive notifications and send outbreak alerts through email messages, SNMP Trap, or Windows Event Log when threats are detected on clients.
- Control outbreaks by configuring and enabling Outbreak Defense.
Opening the Web Console

Before you begin

Open the web console from any client on the network that has the following resources:

• Internet Explorer 6.0 SP2 or later
• High-color display with a resolution of 1024x768 or higher

Procedure

1. Choose one of the following options to open the web console:
   • On the computer that hosts the Security Server, go to the Desktop and click the Worry-Free Business Security shortcut.
   • On any client on the network, open a web browser and type the following in the address bar:

      https://{Security_Server_Name or IP Address}:{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
Tip

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.

If the environment cannot resolve server names by DNS, use the server name instead of the IP address.

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

2. Type your password and click Log on.

The browser displays the Live Status screen.

What to do next

Check the following if you are unable to access the web console.

<table>
<thead>
<tr>
<th>Item To Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>If you have forgotten your password, use the Console Password Reset Tool to reset the password. Access this tool on the Security Server computer under the Trend Micro Worry-Free Business Security folder in the Windows Start menu.</td>
</tr>
<tr>
<td><strong>Browser Cache</strong></td>
<td>If you upgraded from a previous version of WFBS, web browser and proxy server cache files may prevent the web console from loading. Clear the cache memory on your browser and on any proxy servers located between the Trend Micro Security Server and the client you use to access the web console.</td>
</tr>
<tr>
<td><strong>SSL Certificate</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

### Web Console Navigation

#### Web Console Main Sections

The web console contains the following main sections:
A. Main menu

At the top of the web console is the main menu.

At the top right corner is a drop-down box containing shortcuts to tasks that administrators perform frequently.

The Logout link is also provided to allow you to end your current session.

B. Configuration area

Below the main menu items is the configuration area. Use this area to select options according to the menu item you selected.

C. Menu sidebar (not available on all screens)

When you choose a Security Agent group from the Security Settings screen and click Configure, a menu sidebar displays. Use the sidebar to configure security settings and scans for the desktops and servers that belong to the group.

When you choose a Messaging Security Agent from the Security Settings screen (Advanced only), you can use the sidebar to configure security settings and scans for your Microsoft Exchange servers.

**Web Console Menu Options**

Use the following menu options from web console:
### Live Status
Provides a central function in the Worry-Free Business Security strategy. Use Live Status to view alerts and notifications about outbreaks and critical security risks.

- View red or yellow alert warnings issued by Trend Micro
- View the latest threats to clients on your network
- View the latest threats to Microsoft Exchange servers (Advanced only)
- Deploy updates to clients that are at risk

### Security Settings
- Customize security settings for agents
- Replicate settings between groups

### Outbreak Defense
Provides alerts to current status and guides you through an outbreak cycle

### Scans
- Scan clients for threats
- Schedule scanning for clients

### Updates
- Check the Trend Micro ActiveUpdate server (or a custom update source) for the latest updated components, including updates to the virus pattern, scan engine, cleanup components, and the agent program
- Configure update source
- Designate Security Agents as Update Agents

### Reports
Generate reports to keep track of threats and other security-related events
### MENU OPTIONS

<table>
<thead>
<tr>
<th>Preferences</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Set up notifications for abnormal threat-related or system-related events</td>
<td>• Set up global settings for ease of maintenance</td>
</tr>
<tr>
<td>• Use management tools to help manage security for the network and clients</td>
<td>• View product license information, maintain the administrator password, and help keep the business environment safe for the exchange of digital information by joining the Smart Feedback program</td>
</tr>
<tr>
<td>• View product license information, maintain the administrator password,</td>
<td></td>
</tr>
<tr>
<td>• Access the latest information from the Knowledge Base (KB)</td>
<td></td>
</tr>
<tr>
<td>• View Security, Sales, Support, and version information</td>
<td></td>
</tr>
</tbody>
</table>

### Help

<table>
<thead>
<tr>
<th>Help</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Search for specific content and topics</td>
<td></td>
</tr>
<tr>
<td>• View the Administrator’s Guide</td>
<td></td>
</tr>
<tr>
<td>• Access the latest information from the Knowledge Base (KB)</td>
<td></td>
</tr>
<tr>
<td>• View Security, Sales, Support, and version information</td>
<td></td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>ICON</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Help icon" /></td>
<td>Help icon. Opens the online help.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh icon" /></td>
<td>Refresh icon. Refreshes the view of the current screen.</td>
</tr>
<tr>
<td><img src="image" alt="Expand/Collapse section icon" /></td>
<td>Expand/Collapse section icon. Displays/hides sections. You can expand only one section at a time.</td>
</tr>
<tr>
<td><img src="image" alt="Information icon" /></td>
<td>Information icon. Displays information pertaining to a specific item.</td>
</tr>
<tr>
<td><img src="image" alt="Customize notifications icon" /></td>
<td>Customize notifications icon. Displays various notification options.</td>
</tr>
</tbody>
</table>
Live Status

Use the Live Status screen to view the status of the WFBS network. To manually refresh
the screen information, click **Refresh**.

**Understanding Icons**

Icons warn you if any action is necessary. Expand a section to view more information.
You can also click the items in the table to view specific details. To find more
information about specific clients, click the number links that appear in the tables.
### TABLE 2-3. Live Status Icons

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>Normal</td>
</tr>
<tr>
<td></td>
<td>Only a few clients require patching. The virus, spyware, and other malware activity on your computers and network represent an insignificant risk.</td>
</tr>
<tr>
<td>🔴</td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>🟡</td>
<td>Action required</td>
</tr>
<tr>
<td></td>
<td>A warning icon means that the administrator must take action to solve a security issue.</td>
</tr>
</tbody>
</table>

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

**Threat Status**

This section shows the following information:

### TABLE 2-4. Threat Status Sections and Displayed Information

<table>
<thead>
<tr>
<th>SECTION</th>
<th>DISPLAYED INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbreak Defense</td>
<td>A possible virus outbreak on your network.</td>
</tr>
<tr>
<td>SECTION</td>
<td>DISPLAYED INFORMATION</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Starting from the 5th incident, the status icon changes to display the Warning. If you must take action:</td>
</tr>
<tr>
<td></td>
<td>• The Security Agent did not successfully perform the action it was set up to perform. Click the number link to view detailed information about computers on which the Security Agent was unable to perform and take an action.</td>
</tr>
<tr>
<td></td>
<td>• Real-time scanning is disabled on Security Agents. Click <strong>Enable Now</strong> to start Real-time scanning again.</td>
</tr>
<tr>
<td></td>
<td>• The real-time scanning is disabled on the Messaging Security Agent.</td>
</tr>
<tr>
<td>Anti-spyware</td>
<td>Displays the latest spyware scan results and spyware log entries. The <strong>Number of Incidents</strong> 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 <strong>Incidents Detected</strong> column of the Spyware Threat Incidents table. From there, you can find information about the specific spyware threats that are affecting your clients.</td>
</tr>
<tr>
<td>Anti-spam</td>
<td>Click the <strong>High</strong>, <strong>Medium</strong>, or <strong>Low</strong> 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 <strong>Disabled</strong> to be redirected to the appropriate screen. This information is updated on an hourly basis.</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>Potentially dangerous websites as determined by Trend Micro. Starting from the 200th incident, the status icon changes to display a warning.</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Restricted websites as determined by the administrator. Starting from the 300th incident, the status icon changes to display a warning.</td>
</tr>
<tr>
<td>Behavior Monitoring</td>
<td>Violations of the behavior monitoring policies.</td>
</tr>
<tr>
<td>Network Viruses</td>
<td>Detections determined by the firewall settings.</td>
</tr>
<tr>
<td>Device Control</td>
<td>Restricts access to USB devices and network drives.</td>
</tr>
</tbody>
</table>
System Status

This section shows information regarding the updated components and free space on clients where agents are installed.

**Table 2-5. System Status Sections and Displayed Information**

<table>
<thead>
<tr>
<th>SECTION</th>
<th>DISPLAYED INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Updates</td>
<td>The status of component updates for the Security Server or the deployment of updated components to agents.</td>
</tr>
<tr>
<td>Smart Scan</td>
<td>The Security Agents that cannot connect to the Scan Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The Scan Server is a service hosted on the Security Server.</td>
</tr>
<tr>
<td>Unusual system events</td>
<td>Disk space information about clients that are functioning as servers (running server operating systems).</td>
</tr>
</tbody>
</table>

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

License Status

This section shows 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 2-6. Live Status Update Intervals**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>UPDATE INTERVAL (MINUTES)</th>
<th>AGENT SENDS LOGS TO SERVER AFTER... (MINUTES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbreak Defense</td>
<td>3</td>
<td>N/A</td>
</tr>
<tr>
<td>Antivirus</td>
<td>1</td>
<td>Security Agent: Immediate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Messaging Security Agent: 5</td>
</tr>
</tbody>
</table>
### Component Update Intervals

<table>
<thead>
<tr>
<th>Item</th>
<th>Update Interval (Minutes)</th>
<th>Agent Sends Logs to Server After... (Minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-spyware</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Anti-spam</td>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>3</td>
<td>Immediate</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>3</td>
<td>Immediate</td>
</tr>
<tr>
<td>Behavior Monitoring</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Network Virus</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Device Control</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Smart Scan</td>
<td>60</td>
<td>N/A</td>
</tr>
<tr>
<td>License</td>
<td>10</td>
<td>N/A</td>
</tr>
<tr>
<td>Component Updates</td>
<td>3</td>
<td>N/A</td>
</tr>
<tr>
<td>Unusual System Events</td>
<td>10</td>
<td>When the listening service TmListen is started</td>
</tr>
</tbody>
</table>
Chapter 3

Installing Agents

This chapter explains the steps necessary for installing Security Agents and Messaging Security Agents (Advanced only). It also provides information on removing these agents.
Security Agent Installation

Perform a fresh installation of the Security Agent on Windows clients (desktops and servers). Use the installation method that best suit your requirements.

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

Note
For information on upgrading Security Agents to this version, see the Installation and Upgrade Guide.

Security Agent Installation Requirements

Visit the following website for a complete list of installation requirements and compatible third-party products:


Security Agent Installation Considerations

Before installing Security Agents, consider the following:

• **Agent features**: Some Security Agent features are not available on certain Windows platforms. For details, see Available Security Agent Features on page 3-3.

• **x64 platforms**: A scaled down version of the Security Agent is available for the x64 platform. However, no support is currently available for the IA-64 platform.

• **IPv6 support**: The Security Agent can be installed on dual-stack or pure IPv6 clients. However:
  • Some of the Windows operating systems to which the agent can be installed do not support IPv6 addressing.
  • For some of the installation methods, there are special requirements to install the agent successfully.
Installing Agents

For details, see *Security Agent Installation and IPv6 Support on page 3-6*.

- **Exception lists**: Ensure that exception lists for the following features have been configured properly:
  
  - **Behavior Monitoring**: Add critical client applications to the Approved Programs list to prevent the Security Agent from blocking these applications. For more information, see *Configuring Behavior Monitoring on page 5-19*.
  
  - **Web Reputation**: Add websites that you consider safe to the Approved URL List to prevent the Security Agent from blocking access to the websites. For more information, see *Configuring Web Reputation for Security Agents on page 5-16*.
  
  - **Agent installation directory**: During the Security Server installation, Setup prompts you to specify the agent installation directory, which is `$ProgramFiles\Trend Micro\Security Agent` by default. If you want to install the Security Agents to a different directory, specify the new directory in *Preferences > Global Settings > System > Security Agent Installation* section.

### Available Security Agent Features

The Security Agent features available on a client depend on the client’s operating system. Be aware of unsupported features when installing an agent to a particular operating system.

**Table 3-1. Security Agent Features**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Scan, Real-time Scan, and Scheduled Scan</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----</td>
<td>-------</td>
<td>---</td>
<td>---</td>
<td>-----------------</td>
<td>-----------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Web reputation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Behavior Monitoring</td>
<td>Yes (32-bit)</td>
<td>Yes (32/64-bit)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (32-bit)</td>
<td>Yes (32-bit)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Device Control</td>
<td>Yes (32-bit)</td>
<td>Yes (32/64-bit)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (32-bit)</td>
<td>Yes (32-bit)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Damage Cleanup Services</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IM Content Filtering</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Supported IM applications:
- AIM 6
- ICQ 6
- MSN 7.5, 8.1
- Yahoo! Messenger 8.1
## Windows Operating System

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>POP3 mail scan</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual and scheduled updates</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Update Agent</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Agent Plug-in Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Smart Feedback</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trend Micro Anti-spam Toolbar</td>
<td>Yes (32-bit) Yes</td>
<td>Yes (64-bit) Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Supported email clients:
- Outlook Express 6.0 with Service Pack 2 or later
- Windows Mail 6.0
- Windows Live Mail 2011

HouseCall | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
Security Agent Installation and IPv6 Support

This topic discusses considerations when installing the Security Agent to dual-stack or pure IPv6 clients.

**Operating System**

The Security Agent can only be installed on the following operating systems that support IPv6 addressing:

- Windows Vista (all editions)
- Windows Server 2008 (all editions)
- Windows 7 (all editions)
- Windows SBS 2011
- Windows 8 (all editions)
- Windows Server 2012 (all editions)

Visit the following website for a complete list of system requirements:

Supported Installation Methods

All of the available installation methods can be used to install the Security Agent on pure IPv6 or dual-stack clients. For some installation methods, there are special requirements to install the Security Agent successfully.

**Table 3-2. Installation Methods and IPv6 Support**

<table>
<thead>
<tr>
<th><strong>Installation Method</strong></th>
<th><strong>Requirements/Considerations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Web Page and Email Notification Install</td>
<td>If you are installing to a pure IPv6 client, the Security Server must be dual-stack or pure IPv6 and its host name or IPv6 address must be part of the URL. For dual-stack clients, the IPv6 address that displays in the installation status screen depends on the option selected in the <em>Preferred IP Address</em> section in <em>Preferences &gt; Global Settings &gt; Desktop/Server</em> tab.</td>
</tr>
<tr>
<td>Vulnerability Scanner and Remote Install</td>
<td>A pure IPv6 Security Server cannot install the Security Agent on pure IPv4 clients. Similarly, a pure IPv4 Security Server cannot install the agent on pure IPv6 clients.</td>
</tr>
</tbody>
</table>

Security Agent IP Addresses

A Security Server installed in an environment that supports IPv6 addressing can manage the following Security Agents:

- A Security Server installed on a dual-stack client and has been assigned both IPv4 and IPv6 addresses can manage pure IPv6, dual-stack, and pure IPv4 Security Agents.

After you install or upgrade Security Agents, the agents register to the Security Server using an IP address.

- Pure IPv6 Security Agents register using their IPv6 address.
- Pure IPv4 Security Agents register using their IPv4 address.
• Dual-stack Security Agents register using either their IPv4 or IPv6 address. You can choose the IP address that these agents will use in the **Preferred IP Address** section in **Preferences > Global Settings > Desktop/Server** tab.

## Security Agent Installation Methods

This section provides a summary of the different installation methods to perform a fresh installation of the Security Agent. All installation methods require local administrator rights on the target clients.

If you are installing Security Agents and want to enable IPv6 support, read the guidelines in *Security Agent Installation and IPv6 Support on page 3-6*.

### TABLE 3-3. Installation Methods

<table>
<thead>
<tr>
<th><strong>INSTALLATION METHOD/ OPERATING SYSTEM SUPPORT</strong></th>
<th><strong>DEPLOYMENT CONSIDERATIONS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Web Page</td>
<td><strong>DEPLOYMENT</strong></td>
</tr>
<tr>
<td>Supported on all operating systems</td>
<td>Yes</td>
</tr>
<tr>
<td>Email Notification</td>
<td>Yes</td>
</tr>
<tr>
<td>INSTALLATION METHOD/ OPERATING SYSTEM SUPPORT</td>
<td>DEPLOYMENT CONSIDERATIONS</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td>WAN DEPLOYMENT</td>
</tr>
<tr>
<td>Remote Install</td>
<td>No</td>
</tr>
<tr>
<td>Supported on all operating systems except:</td>
<td></td>
</tr>
<tr>
<td>• Windows Vista Home Basic and Home Premium Editions</td>
<td></td>
</tr>
<tr>
<td>• Windows XP Home Edition</td>
<td></td>
</tr>
<tr>
<td>• Windows 7 Home Basic/ Home Premium</td>
<td></td>
</tr>
<tr>
<td>Login Script Setup</td>
<td>No</td>
</tr>
<tr>
<td>Supported on all operating systems</td>
<td></td>
</tr>
<tr>
<td>Client Packager</td>
<td>Yes</td>
</tr>
<tr>
<td>INSTALLATION METHOD/OPERATING SYSTEM SUPPORT</td>
<td>DEPLOYMENT CONSIDERATIONS</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td></td>
<td>WAN DEPLOYMENT</td>
</tr>
<tr>
<td>Trend Micro Vulnerability Scanner (TMVS)</td>
<td>No</td>
</tr>
</tbody>
</table>

Supported on all operating systems except:

- Windows Vista Home Basic and Home Premium Editions
- Windows XP Home Edition
- Windows 7 Home Basic/ Home Premium

For single-site deployment and in organizations where IT policies are strictly enforced, IT administrators can choose to deploy using **Remote Install** or **Login Script Setup**.

In organizations where IT policies are less strictly enforced, Trend Micro recommends installing Security Agents using the **Internal Web Page**. Using this method, however, requires that end users who will install the Security Agent to have administrator privileges.

**Remote Install** is efficient for networks with Active Directory. If your network does not use Active Directory, use the Internal Web Page.

### Installing from the Internal Web Page

#### Before you begin

To install from the Internal Web Page, the following are required:
### Item to Check | Requirement
--- | ---
Security Server | The Security Server must be installed on:
| • Windows XP, Vista, 7, 8, Server 2003/2008/2012, or SBS 2011
| • with Internet Information Server (IIS) 6.0, 7.0, 7.5, 8.0 or Apache 2.0.6x
Target client | • The target client must have Internet Explorer 6.0 or later.
| • Users must use an administrator account to log on to the client.

**Note**
If the target client runs Windows 7, enable the built-in administrator account first. Windows 7 disables the built-in administrator account by default. For more information, refer to the Microsoft support site ([http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx](http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx)).

Target client running Windows XP, Vista, Server 2008, 7, 8, SBS 2011, Server 2012 | Users must perform the following steps:
1. Launch Internet Explorer and add the Security Server URL (such as `https://<Security Server name>:4343/SMB/console/html/client`) to the list of trusted sites. On Windows XP, access the list by going to **Tools > Internet Options > Security** tab, selecting the **Trusted Sites** icon, and clicking **Sites**.
2. Modify the Internet Explorer security setting to enable **Automatic prompting for ActiveX controls**. On Windows XP, go to **Tools > Internet Options > Security** tab, and click **Custom level**.

Target client running Windows Vista | Users must enable Protected Mode. To enable Protected Mode, in Internet Explorer, click **Tools > Internet Options > Security** tab.

IPv6 | If you have a mixed environment consisting of pure IPv4, pure IPv6, and dual-stack clients, the Security Server must have both IPv4 and IPv6 addresses so that all clients can connect to the Internal Web Page on the Security Server.
Send the following instructions to users to install the Security Agent from the Internal Web Page. To send an installation notification through email, see Installing with Email Notification on page 3-31.

**Procedure**

1. Log on to the client using an administrator account.
2. Open an Internet Explorer window and type one of the following:
   - Security Server with SSL:
     
     https://<Security Server name or IP Address>:4343/SMB/console/html/client
   - Security Server without SSL:
     
     http://<Security Server name or IP Address>:8059/SMB/console/html/client
3. Click **Install Now** to start installing the Security Agent.

   The installation starts. Allow ActiveX control installation when prompted. The Security Agent icon appears in the Windows Task Bar after installation.

   **Note**

   For a list of icons that display on the Windows Task Bar, see Checking the Security Agent Status on page A-2.

**What to do next**

If users report that they cannot install from the Internal Web Page, 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 if the proxy settings are configured correctly.
• In the web browser, delete Trend Micro add-ons and the browsing history.

**Installing with Login Script Setup**

Login Script Setup automates the installation of the Security Agent to unprotected clients when they log on to the network. Login Script Setup adds a program called *AutoPcc.exe* to the server login script.

*AutoPcc.exe* installs the Security Agent to unprotected clients and updates program files and components. Clients must be part of the domain to be able to use *AutoPcc* through the login script.

If you already have an existing login script, Login Script Setup appends a command that executes *AutoPcc.exe*. Otherwise, it creates a batch file called *ofcscan.bat* that contains the command to run *AutoPcc.exe*.

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

```
\\<Server_name>\ofcscan\autopcc
```

Where:

- `<Server_name>` is the computer name or IP address of the Security Server computer.
- "ofcscan" is the shared folder name on the Security Server.
- "autopcc" is the link to the autopcc executable file that installs the Security Agent.

Login script location on all Windows Server versions (through a net logon shared directory):

```
\\Windows server\system drive\windir\sysvol\domain\scripts ofcscan.bat
```

**Procedure**

1. On the computer you used to run the server installation, open `<Security Server installation folder>\PCCSRV\Admin.`
2. Double-click SetupUsr.exe. The Login Script Setup utility loads. The console displays a tree showing all domains on the network.

3. Locate the server whose login script you want to modify, select it, and then click Select. Ensure that the server is a primary domain controller and that you have administrator access to the server.

Login Script Setup prompts you for a user name and password.

4. Type the user name and password. Click OK to continue.

The User Selection screen appears. The Users list shows the profiles of users that log on to the server. The Selected users list shows the user profiles whose login script you want to modify.

5. To modify the login script for a user profile, select the user profile from the Users list, and then click Add.

6. To modify the login script of all users, click Add All.

7. To exclude a user profile that you previously selected, select the name from the Selected users list, and click Delete.

8. To reset your choices, click Delete All.

9. Click Apply when all target user profiles are in the Selected users list.

A message informs you that you have modified the server login scripts successfully.

10. Click OK.

Login Script Setup returns to its initial screen.

11. To close Login Script Setup, click Exit.

---

**Installing with Client Packager**

Client Packager creates an installation package that you can send to users using conventional media such as CD-ROM. Users run the package on the client to install or upgrade the Security Agent and update components.
Client Packager is especially useful:

- When deploying the Security Agent or components to clients in low-bandwidth remote offices.
- If your environment has restrictions connecting to the Internet, in the case of a closed LAN or lack of an Internet connection.

Security Agents installed using Client Packager report to the server where the package was created.

### Procedure

1. On the Security Server computer, browse to `<Server installation folder>\PCCSRV\Admin\Utility\ClientPackager`.

2. Double-click `ClnPack.exe`.

   The Client Packager console opens.

3. Select the operating system for which you want to create the package. Deploy the package only to clients that run the operating system type. Create another package to deploy to another operating system type.

4. Select the scan method for the package.

   For details about scan methods, see *Scan Methods on page 5-3.*

   The components included in the package depend on the scan method you have selected. For smart scan, all components, except Virus Pattern, will be included. For conventional scan, all components, except Smart Scan Agent Pattern, will be included.

5. Select the type of package you want to create.
### Table 3-4. Client Package Types

<table>
<thead>
<tr>
<th>Package Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td>Select <strong>Setup</strong> to create the package as an MSI file, which conforms to the Microsoft Installer Package format. The package installs the Security Agent program with the components currently available on the Security Server. If the target client has an earlier Security Agent version installed and you want to upgrade, create the MSI file from the Security Server that manages the agent. Otherwise, the agent will not be upgraded.</td>
</tr>
<tr>
<td>Update</td>
<td>Select <strong>Update</strong> to create a package that contains the components currently available on the Security Server. The package will be created as an executable file. Use this package if there are issues updating components on the client where the Security Agent is installed.</td>
</tr>
</tbody>
</table>

6. Click **Silent mode** to create a package that installs on the client in the background, unnoticeable to the client user and without showing an installation status window. Enable this option if you plan to deploy the package remotely to the client.

7. Click **Disable prescan (only for fresh install)** if you do not want to scan the client for threats before installing the Security Agent. Do this if you are certain that the client is threat-free.

   If prescan is enabled, Setup scans for virus/malware in the most vulnerable areas of the computer, which include the following:
   - Boot area and boot directory (for boot viruses)
   - Windows folder
   - Program files folder

8. Next to **Source file**, ensure that the location of the `ofcscan.ini` file is correct. To modify the path, click (…) to browse for the `ofcscan.ini` file. By default, this file is in `<Server installation folder>\PCCSRV`.

9. In Output file, click (…), specify where you want to create the package, and type the package file name (for example, `ClientSetup.exe`).
10. Click **Create**.

After Client Packager creates the package, the message “Package created successfully” appears. Locate the package in the directory that you specified in the previous step.

**What to do next**

Deploy the package to clients.

**Client Requirements:**

- 1GB free disk space if the scan method for the package is conventional scan, 500MB if smart scan
- Windows Installer 3.0 (to run an MSI package)

**Package Deployment Guidelines:**

- Send the package to users and ask them to run the package by double-clicking the file (.msi or .exe).

**Note**

Send the package only to users whose Security Agent will report to the server where the package was created.

- If you have users who will run the .exe package on computers running Windows Vista, 7, 8, Server 2008, SBS 2011, or Server 2012, instruct them to right-click the .exe file and select **Run as administrator**.

- If you are using Active Directory, you can automatically deploy the Security Agent to all clients simultaneously with the .msi file, rather than requiring each user to install the Security Agent themselves. Use **Computer Configuration** instead of **User Configuration** so that the Security Agent can be installed regardless of which user logs on to the client.

- If a newly installed Security Agent cannot connect to the Security Server, the Security Agent will keep default settings. When the Security Agent connects to the Security Server, it will obtain the settings for its group in the web console.

- If you encounter problems upgrading the Security Agent with Client Packager, Trend Micro recommends uninstalling the previous version of the Security Agent.
first, then installing the new version. For uninstallation instructions, see *Removing Agents* on page 3-37.

### Installing with Remote Install

#### Before you begin

Install the Security Agent remotely to one or several clients connected to the network.

To install with Remote Install, the following are required:

<table>
<thead>
<tr>
<th><strong>Item to Check</strong></th>
<th><strong>Requirement</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Target client</td>
<td>Use an administrator account to log on to each target client.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If the target client runs Windows 7, enable the built-in administrator account first. Windows 7 disables the built-in administrator account by default. For more information, refer to the Microsoft support site (<a href="http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx">http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx</a>).</td>
</tr>
<tr>
<td></td>
<td>The target client must not have Security Server installed. Remote Install does not install the Security Agent on a client already running the Security Server.</td>
</tr>
</tbody>
</table>
Target client running Windows Vista, 7, 8, Server 2008/2012, or SBS 2011

<table>
<thead>
<tr>
<th>ITEM TO CHECK</th>
<th>REQUIREMENT</th>
</tr>
</thead>
</table>
| Target client running Windows Vista, 7, 8, Server 2008/2012, or SBS 2011 | Perform the following tasks:  
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.  

| Note | Type services.msc in the Run window to open Microsoft Management Console.  

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

IPv6 | A dual-stack Security Server can install the Security Agent to any client. A pure IPv6 Security Server can only install the Security Agent to pure IPv6 or dual-stack clients. |
Procedure

1. In the web console, navigate to Security Settings > Add.
   
   A new screen opens.

2. Select Desktop or Server, from the Computer Type section.

3. Select Remote Install, from the Method section.

4. Click Next.
   
   A new screen appears.

5. From the list of clients in the Groups and Computers box, select a client, and then click Add. A prompt for a user name and password to the client appears.

6. Type your user name and password, and then click Login. The client appears in the Selected Computers list box.

7. Repeat these steps until the list displays all the clients in the Selected Computer list box.

8. Click Install.
   
   A confirmation box appears.

9. Click Yes to confirm that you want to install the agent to the clients.
   
   A progress screen appears as the program copies the Security Agent files to each client.

   When the Security Server completes the installation to a client, the installation status will appear in the Result field of the Selected Computers list box, and the client name appears with a green check mark.

What to do next

If installation with remote install is unsuccessful, perform these tasks:

• Verify that client-server communication exists by using ping and telnet.

• Check if TCP/IP on the client is enabled and properly configured.
If you are using a proxy server for client-server communication, check if the proxy settings are configured correctly.

In the web browser, delete Trend Micro add-ons and the browsing history.

Installing with Vulnerability Scanner

Before you begin

Run vulnerability scans to detect installed antivirus solutions, search for unprotected clients on the network, and install Security Agents to clients.

To install with Vulnerability Scanner, the following are required:

<table>
<thead>
<tr>
<th>Item to Check</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where to launch Vulnerability Scanner</td>
<td>You can launch Vulnerability Scanner on the Security Server or on any client in the network. The client should not be running Terminal Server.</td>
</tr>
</tbody>
</table>
| Target client                 | • The target client must not have Security Server installed. Vulnerability Scanner does not install the Security Agent on a client already running the Security Server.  
                                 | • Users must use an administrator account to log on to the client. |

**Note**

If the target client runs Windows 7, enable the built-in administrator account first. Windows 7 disables the built-in administrator account by default. For more information, refer to the Microsoft support site (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).

There are several ways to run vulnerability scans.

• **Running a Manual Vulnerability Scan on page 3-22**

• **Running a DHCP Scan on page 3-23**

• **Configuring a Scheduled Vulnerability Scan on page 3-25**
Running a Manual Vulnerability Scan

Run vulnerability scans on demand.

Procedure

1. Launch Vulnerability Scanner.

<table>
<thead>
<tr>
<th>TO LAUNCH VULNERABILITY SCANNER ON:</th>
<th>STEPS</th>
</tr>
</thead>
</table>
| The Security Server                | a. Navigate to `<Server installation folder>\PCCSRV\Admin\Utility\TMVS.`  
  b. Double-click TMVS.exe. |
| A client on the network             | a. On the Security Server, navigate to `<Server installation folder>\PCCSRV\Admin\Utility.`  
  b. Copy the TMVS folder to the other client.  
  c. On the other client, open the TMVS folder and then double-click TMVS.exe. |

2. Go to the Manual Scan section.

3. Type the IP address range of the clients you want to check.
   a. Type an IPv4 address range.
      
      Note
      Vulnerability Scanner can only query an IPv4 address range if it runs on a pure IPv4 or dual-stack client. Vulnerability Scanner only supports a class B IP address range, for example, 168.212.1.1 to 168.212.254.254.

      b. For an IPv6 address range, type the IPv6 prefix and length.

      Note
      Vulnerability Scanner can only query an IPv6 address range if it runs on a pure IPv6 or dual-stack client.
4. Click **Settings**.

   The **Settings** screen appears.

5. Configure vulnerability scan settings. For details, see *Vulnerability Scan Settings on page 3-28*.

6. Click **OK**.

   The Settings screen closes.

7. Click **Start**.

   The vulnerability scan results appear in the **Results** table under the **Manual Scan** tab.

8. To save the results to a comma-separated value (CSV) file, click **Export**, locate the folder where you want to save the file, type the file name, and click **Save**.

---

**Running a DHCP Scan**

Run vulnerability scans on clients requesting IP addresses from a DHCP server.

Vulnerability Scanner listens on port 67, which is the DHCP server’s listening port for DHCP requests. If it detects a DHCP request from a client, vulnerability scan runs on the client.

---

**Note**

Vulnerability Scanner is unable to detect DHCP requests if you launched it on Windows Server 2008 or Windows 7.
Procedure

1. Configure DHCP settings in the TMVS.ini file found under the following folder:
   \{Server installation folder}\PCCSRV\Admin\Utility\TMVS.

   **Table 3-5. DHCP Settings in the TMVS.ini File**

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>DhcpThreadNum=x</td>
<td>Specify the thread number for DHCP mode. The minimum is 3, the maximum is 100. The default value is 3.</td>
</tr>
<tr>
<td>DhcpDelayScan=x</td>
<td>This is the delay time in seconds before checking the requesting computer for installed antivirus software. The minimum is 0 (do not wait) and the maximum is 600. The default value is 60.</td>
</tr>
<tr>
<td>LogReport=x</td>
<td>0 disables logging, 1 enables logging. Vulnerability Scanner sends the results of the scan to the WFBS server. Logs display in the <strong>System Event Logs</strong> screen on the web console.</td>
</tr>
<tr>
<td>OsceServer=x</td>
<td>This is the WFBS server’s IP address or DNS name.</td>
</tr>
<tr>
<td>OsceServerPort=x</td>
<td>This is the web server port on the WFBS server.</td>
</tr>
</tbody>
</table>

2. Launch Vulnerability Scanner.

   **Table: To Launch Vulnerability Scanner On**

<table>
<thead>
<tr>
<th>TO LAUNCH VULNERABILITY SCANNER ON:</th>
<th>STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Security Server</td>
<td>a. Navigate to {Server installation folder}\PCCSRV\Admin\Utility\TMVS.</td>
</tr>
<tr>
<td></td>
<td>b. Double-click TMVS.exe.</td>
</tr>
</tbody>
</table>
3. Next to the Manual Scan section, click Settings. The Settings screen appears.

4. Configure vulnerability scan settings. For details, see Vulnerability Scan Settings on page 3-28.

5. Click OK. The Settings screen closes.

6. In the Results table, click the DHCP Scan tab.

   **Note**

   The DHCP Scan tab is not available on computers running Windows Server 2008 and Windows 7.

7. Click DHCP Start.

   Vulnerability Scanner begins listening for DHCP requests and performing vulnerability checks on clients as they log on to the network.

8. To save the results to a comma-separated value (CSV) file, click Export, locate the folder where you want to save the file, type the file name, and click Save.

### Configuring a Scheduled Vulnerability Scan

Vulnerability scans automatically run according to a schedule.
Procedure

1. Launch Vulnerability Scanner.

<table>
<thead>
<tr>
<th><strong>To Launch Vulnerability Scanner On:</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
</table>
| The Security Server                    | a. Navigate to `<Server installation folder>\PCCSRV\Admin\Utility\TMVS`.  
b. Double-click TMVS.exe. |
| A client on the network                 | a. On the Security Server, navigate to `<Server installation folder>\PCCSRV\Admin\Utility`.  
b. Copy the TMVS folder to the other client.  
c. On the other client, open the TMVS folder and then double-click TMVS.exe. |

2. Go to the Scheduled Scan section.

3. Click Add/Edit.

   The Scheduled Scan screen appears.

4. Type a name for the scheduled vulnerability scan.

5. Type the IP address range of the computers you want to check.
   a. Type an IPv4 address range.
      b. For an IPv6 address range, type the IPv6 prefix and length.

---

**Note**

Vulnerability Scanner can only query an IPv4 address range if it runs on a pure IPv4 or dual-stack host machine that has an available IPv4 address.  
Vulnerability Scanner only supports a class B IP address range, for example, 168.212.1.1 to 168.212.254.254.
Installing Agents

Note
Vulnerability Scanner can only query an IPv6 address range if it runs on a pure IPv6 or dual-stack host machine that has an available IPv6 address.

6. Specify the start time using the 24-hour clock format and then select how often the scan will run. Choose from daily, weekly, or monthly.

7. Select Use current settings if you have configured and want to use manual vulnerability scan settings. For details about manual vulnerability scan settings, see Running a Manual Vulnerability Scan on page 3-22.

If you did not specify manual vulnerability scan settings or if you want to use another set of settings, select Modify settings and then click Settings. The Settings screen appears. Configure scan settings and then click OK. For details, see Vulnerability Scan Settings on page 3-28.

8. Click OK.

The Scheduled Scan screen closes. The scheduled vulnerability scan you created appears under the Scheduled Scan section. If you enabled notifications, Vulnerability Scanner sends you the scheduled vulnerability scan results.

9. To execute the scheduled vulnerability scan immediately, click Run Now.

The vulnerability scan results appear in the Results table under the Scheduled Scan tab.

Note
MAC address information does not display in the Results table if the computer runs Windows Server 2008.

10. To save the results to a comma-separated value (CSV) file, click Export, locate the folder where you want to save the file, type the file name, and click Save.

11. To stop running scheduled vulnerability scans, go to the Scheduled Scans section, select the scheduled scan, and click Delete.
**Vulnerability Scan Settings**

Configure the following settings when running vulnerability scans. For details about the different types of vulnerability scans, see *Installing with Vulnerability Scanner on page 3-21.*

<table>
<thead>
<tr>
<th>SETTINGS</th>
<th>DESCRIPTION AND INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Query</td>
<td>Vulnerability Scanner can check for the presence of security software on the target clients.</td>
</tr>
<tr>
<td></td>
<td>1. Select the security software to check.</td>
</tr>
<tr>
<td></td>
<td>2. Vulnerability Scanner uses the default ports displayed on screen to check for the software. If the software administrator changed the default ports, make the necessary changes or Vulnerability Scanner will not detect the software.</td>
</tr>
<tr>
<td></td>
<td>3. For Norton Antivirus Corporate Edition, you can change the timeout settings by clicking <strong>Settings</strong>.</td>
</tr>
</tbody>
</table>

**Other Product Query Settings**

To set the number of clients that Vulnerability Scanner simultaneously checks for security software:

1. **Navigate to** `<Server installation folder>\PCCSRV \Admin\Utility\TMVS` and open **TMVS.ini** using a text editor such as Notepad.

2. To set the number of clients checked:
   - For manual vulnerability scans, change the value for **ThreadNumManual**. Specify a value between 8 and 64.
     For example, type `ThreadNumManual=60` if you want Vulnerability Scanner to check 60 clients at the same time.
   - For scheduled vulnerability scans, change the value for **ThreadNumSchedule**. Specify a value between 8 and 64.
     For example, type `ThreadNumSchedule=50` if you want Vulnerability Scanner to check 50 clients at the same time.

3. **Save** **TMVS.ini**.
### Description and Instructions

**Description**

When Vulnerability Scanner is able to "ping" clients, it can retrieve additional information about the clients. There are two methods for retrieving information:

- **Normal retrieval**: Retrieves both domain and computer information
- **Quick retrieval**: Retrieves only the computer name

**Alert Settings**

To automatically send the Vulnerability Scan results to yourself or to other administrators in your organization:

1. Select **Email results to the system administrator**.
2. Click **Configure** to specify email settings.
3. In **To**, type the email address of the recipient.
4. In **From**, type the email address of the sender.
5. In **SMTP server**, type the SMTP server address.
   
   For example, type `smtp.company.com`. The SMTP server information is required.
6. In **Subject**, type a new subject for the message or accept the default subject.
7. Click **OK**.

To inform users that their computers do not have security software installed:

1. Select **Display a notification on unprotected computers**.
2. Click **Customize** to configure the notification message.
3. In the **Notification Message** screen, type a new message or accept the default message.
4. Click **OK**.

**Save as CSV File**

Save the vulnerability scan results to a comma-separated value (CSV) file.

The file will be saved on the client where Vulnerability Scanner was launched. Accept the default file path or change it according to your preference.

---

<table>
<thead>
<tr>
<th><strong>Settings</strong></th>
<th><strong>Description and Instructions</strong></th>
</tr>
</thead>
</table>
| Description Retrieval Settings | When Vulnerability Scanner is able to "ping" clients, it can retrieve additional information about the clients. There are two methods for retrieving information:  
- **Normal retrieval**: Retrieves both domain and computer information  
- **Quick retrieval**: Retrieves only the computer name |
| Alert Settings                | To automatically send the Vulnerability Scan results to yourself or to other administrators in your organization:  
1. Select **Email results to the system administrator**.  
2. Click **Configure** to specify email settings.  
3. In **To**, type the email address of the recipient.  
4. In **From**, type the email address of the sender.  
5. In **SMTP server**, type the SMTP server address.  
   
   For example, type `smtp.company.com`. The SMTP server information is required.  
6. In **Subject**, type a new subject for the message or accept the default subject.  
7. Click **OK**.  
To inform users that their computers do not have security software installed:  
1. Select **Display a notification on unprotected computers**.  
2. Click **Customize** to configure the notification message.  
3. In the **Notification Message** screen, type a new message or accept the default message.  
4. Click **OK**. |
| Save as CSV File              | Save the vulnerability scan results to a comma-separated value (CSV) file.  
The file will be saved on the client where Vulnerability Scanner was launched. Accept the default file path or change it according to your preference. |
### Ping Settings

Use "ping" settings to validate the existence of a client and determine its operating system. If these settings are disabled, Vulnerability Scanner scans all the IP addresses in the specified IP address range – even those that are not used on any client – thereby making the scanning attempt longer than it should be.

1. In the **Packet size** and **Timeout** fields, accept or modify the default values.

2. Select **Detect the type of operating system using ICMP OS fingerprinting**.

   If you select this option, Vulnerability Scanner determines if a client runs Windows or another operating system. For clients running Windows, Vulnerability Scanner can identify the version of Windows.

### Other Ping Settings

To set the number of clients that Vulnerability Scanner simultaneously pings:

1. Navigate to `<Server installation folder>\PCCSRV \Admin\Utility\TMVS` and open `TMVS.ini` using a text editor such as Notepad.

2. 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 clients at the same time.

3. Save `TMVS.ini`.

<table>
<thead>
<tr>
<th>SETTINGS</th>
<th>DESCRIPTION AND INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping Settings</td>
<td>Use &quot;ping&quot; settings to validate the existence of a client and determine its operating system. If these settings are disabled, Vulnerability Scanner scans all the IP addresses in the specified IP address range – even those that are not used on any client – thereby making the scanning attempt longer than it should be.</td>
</tr>
<tr>
<td></td>
<td>1. In the <strong>Packet size</strong> and <strong>Timeout</strong> fields, accept or modify the default values.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Detect the type of operating system using ICMP OS fingerprinting</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you select this option, Vulnerability Scanner determines if a client runs Windows or another operating system. For clients running Windows, Vulnerability Scanner can identify the version of Windows.</td>
</tr>
<tr>
<td>Other Ping Settings</td>
<td>To set the number of clients that Vulnerability Scanner simultaneously pings:</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <code>&lt;Server installation folder&gt;\PCCSRV \Admin\Utility\TMVS</code> and open <code>TMVS.ini</code> using a text editor such as Notepad.</td>
</tr>
<tr>
<td></td>
<td>2. Change the value for <strong>EchoNum</strong>. Specify a value between 1 and 64.</td>
</tr>
<tr>
<td></td>
<td>For example, type <code>EchoNum=60</code> if you want Vulnerability Scanner to ping 60 clients at the same time.</td>
</tr>
<tr>
<td></td>
<td>3. Save <code>TMVS.ini</code>.</td>
</tr>
</tbody>
</table>
Installing with Email Notification

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

Procedure

1. In the web console, navigate to Security Settings > Add.

   A new screen opens.

2. Select Desktop or Server, from the Computer Type section.

3. Select Email notification install, from the Method section.

4. Click Next.

   A new 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.
Migrating to the Security Agent

When you install the Security Agent, Setup checks for any Trend Micro or third-party endpoint security software installed on the client.

Setup can perform the following actions:

• Remove other endpoint security software currently installed on the client and then replace it with the Security Agent
• Detect other endpoint security software, but not remove

Visit the following website for a list of endpoint security software:


If the software on the client cannot be removed automatically or can only be detected but not removed, manually uninstall it first. Depending on the uninstallation process of the software, the client may or may not need to restart after uninstallation.

Migration Issues and Possible Solutions

Automatic uninstallation of third-party endpoint security software may be unsuccessful for the following reasons:

• 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.

Possible solutions to these issues:

• Manually remove the third-party software.
• Stop the service for the third-party software.
• Unload the service or process for the third-party software.
Performing Post-installation Tasks on Security Agents

Procedure

1. Verify the following:
   - The Security Agent shortcuts appear on the Windows Start menu on the client.
   - **Trend Micro Worry-Free Business Security Agent** is listed on the Add/Remove Programs list on the client’s Control Panel.
   - The Security Agent appears in the Security Settings screen on the web console and is grouped in the Servers (default) or Desktops (default) group, depending on the client’s operating system type.

   **Note**
   If you do not see the Security Agent, run a connection verification task from Preferences > Global Settings > System (tab) > Agent Connection Verification.

   - The following Security Agent services display on Microsoft Management Console:
     - Trend Micro Security Agent Listener (tmlisten.exe)
     - Trend Micro Security Agent RealTime Scan (ntrtscan.exe)
     - Trend Micro Security Agent NT Proxy Service (TmProxy.exe)

   **Note**
   This service is not available on Windows 8 and Windows Server 2012.

   - Trend Micro Security Agent Firewall (TmPfw.exe) if the firewall was enabled during installation
   - Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe) if Behavior Monitoring or Device Control was enabled during installation
2. If the Security Agent does not appear on the web console, it is possible that it was unable to send its status to the server. Perform any of the following steps:

- 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 agent 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 agent.

- 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.

3. Test the Security Agent using 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.

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

   [http://www.eicar.org/anti_virus_test_file.htm](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`:

   ```
   X50!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.
Installing Agents

Messaging Security Agent Installation

Messaging Security Agents can only be installed if you have the Advanced version of Worry-Free Business Security.

Perform a fresh installation of the Messaging Security Agent on Microsoft Exchange servers.

Note

For information on upgrading Messaging Security Agents to this version, see the Installation and Upgrade Guide.

Messaging Security Agent Installation Requirements

Visit the following website for a complete list of installation requirements:


Installing the Messaging Security Agent (Advanced only)

Before you begin

Installation Notes and Reminders:

- You do not need to stop or start Microsoft Exchange services before or after the installation.

- If information from a previous Messaging Security Agent installation exists on the client, you will be unable to install Messaging Security Agent successfully. Use the Windows Installer Cleanup Utility to clean up remnants of the previous installation. To download the Windows Installer Cleanup Utility, visit:

  http://support.microsoft.com/kb/290301/en-us

- If you are installing the Messaging Security Agent on a server that is running lockdown tools, remove the lockdown tool so that it does not disable the IIS service and causes the installation to fail.
• The Messaging Security Agent can also be installed during the installation of the Security Server. For details, see the Installation and Upgrade Guide.

---

**Procedure**

1. Navigate to **Security Settings > Add.**
   
   A new screen opens.

2. Select **Exchange server.**

3. Under **Exchange Server Information**, type the following information:
   
   • **Server name:** The name of the Microsoft Exchange server to which you want to install the agent.
   
   • **Account:** The built-in domain administrator user name.
   
   • **Password:** The built-in domain administrator password.

4. Click **Next.**

   The installation wizard displays a screen depending on the type of installation you need to do.

   • **Fresh installation:** The agent does not exist on the Microsoft Exchange server and will be installed.

   • **Upgrade:** A previous version of the agent exists on the Microsoft Exchange server and will be upgraded to the current version.

   • **No installation required:** The current version of the agent exists on the Microsoft Exchange server. If the agent does not currently appear in the Security Groups Tree, it will automatically be added.

   • **Invalid:** There is a problem installing the agent.

---

**Note**

For the **Spam Management Type**, **End User Quarantine** will be used.

5. Under **Directories**, change or accept the default target and shared directories for the Messaging Security Agent installation. The default target and shared directories
are C:\Program Files\Trend Micro\Messaging Security Agent and C$, respectively.

6. Click Next.

A new screen opens.

7. Verify that the Microsoft Exchange server settings that you specified in the previous screens are correct, and then click Next to start the installation.

8. To view the status of the installation, click the Live Status tab.

Removing Agents

There are two ways to remove Security Agents and Messaging Security Agents (Advanced only):

Remove Agents from the Web Console

Use this option for inactive agents. An inactive agent continuously appears as offline on the web console because the client on which the agent is installed may have been powered off for a long time or reformatted before the agent can be uninstalled.

When you remove agents from the web console:

• The agent, if it still exists on the client, will not be uninstalled.

• The server stops managing the agent.

• When the agent starts communicating with the server again (for example, after powering on the client), the agent is added back to the web console. A Security Agent applies the settings of its original group. If the group no longer exists, the agent will be grouped under Servers (default) or Desktops (default), depending on the client’s operating system, and apply the settings of that group.
Tip

WFBS provides another feature that checks for and removes inactive agents from the web console. Use this feature to automate the agent removal task. To use this feature, navigate to Preferences > Global Settings > System tab and go to the Inactive Security Agent Removal section.

Uninstall the Agent

You can uninstall the agent (and consequently remove it from the web console) if you encounter problems with the agent program. Trend Micro recommends reinstalling the agent immediately to keep the client protected from threats.

Removing Agents from the Web Console

Procedure

1. Navigate to Security Settings.

2. To remove Security Agents, select a group and then select the agents. To remove a Messaging Security Agent, select it.

Tip

To select multiple, adjacent Security Agents, click the first agent in the range, hold down the SHIFT key, and then click the last agent in the range. To select a range of non-contiguous agents, click the first agent in the range, hold down the CTRL key, and then click the agents you want to select.

3. Click Remove.

   A new screen appears.

4. Click Remove the selected agent(s).

5. Click Apply.
Uninstalling Agents from the Web Console

When uninstalling the Messaging Security Agent, the IIS Admin service/Apache server and all related services will automatically be stopped and restarted.

Procedure

1. Navigate to **Security Settings**.

2. To uninstall Security Agents, select a group and then select the agents. To uninstall a Messaging Security Agent, select it.

   **Tip**
   
   To select multiple, adjacent Security Agents, click the first agent in the range, hold down the SHIFT key, and then click the last agent in the range. To select a range of non-contiguous agents, click the first agent in the range, hold down the CTRL key, and then click the agents you want to select.

3. Click **Remove**.

   A new screen appears.

4. Click **Uninstall the selected agent(s)**.

5. Click **Apply**.

   A popup screen appears and displays the number of uninstall notifications that were sent by the server and the number of agents that received the notification.

   **Note**
   
   For a Messaging Security Agent, type the corresponding Microsoft Exchange server account name and password when prompted.

6. Click **OK**.

7. To verify that the agent has been uninstalled, refresh the Security Settings screen. The agent should no longer appear on the Security Groups Tree.
If the Security Agent uninstallation fails, see *Using the SA Uninstall Tool on page 3-40*.

### Uninstalling the Security Agent from the Client

Users can uninstall the agent from the client.

Depending on your configuration, uninstallation may or may not require a password. If a password is required, ensure that you share the password only to users that will run the uninstallation program and then change the password immediately if it has been divulged to other users.

The password can be set or disabled at **Preferences > Global Settings > Desktop/Server tab > Security Agent Uninstallation Password**.

**Procedure**

1. Click **Control Panel > Add or Remove Programs**.
2. Locate **Trend Micro Worry-Free Business Security Agent** and click **Change** or **Uninstall**, whichever is available.
3. Follow the on-screen instructions.
4. If prompted, type the uninstallation password.
   
   The Security Server notifies the user of the uninstallation progress and completion. The user does not need to restart the client to complete the uninstallation.

   In the event this procedure fails, see *Using the SA Uninstall Tool on page 3-40*.

### Using the SA Uninstall Tool

Use the SA Uninstall Tool:

- When an installation fails or a complete uninstall is needed. The tool automatically removes all Security Agent components from a client.
- To unload the Security Agent
**Procedure**

1. On the Security Server, navigate to `<Server installation folder>\PCCSRV\Private`.
2. Copy the `SA_Uninstall.exe` file to the target client.
4. Log on to Windows as Administrator (or any account with Administrator privileges).
5. Follow the steps for the task that you wish to perform.

<table>
<thead>
<tr>
<th><strong>Task</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
</table>
| Uninstall the Security Agent | a. Run `Uninstall.bat`. There are several ways to perform this step.  
  • On Windows Vista, 7, 8, Server 2008/2012, or SBS 2011, navigate to the tool’s directory, right-click `Uninstall.bat`, and select **Run as Administrator**. At the UAC screen, select **Agree**.  
  • On Windows XP/2003, double-click `Uninstall.bat`.  
  b. When the message **Do you want to reboot now? (Y/N)** appears, select either:  
  • **N [Enter]**: Some drivers will not be uninstalled until you reboot.  
  • **Y [Enter]**: Reboot occurs after a 30-second countdown. 
    The SA Uninstall Tool automatically stops the agent. |
Uninstalling the Messaging Security Agent from the Microsoft Exchange Server (Advanced Only)

When uninstalling the Messaging Security Agent, the IIS Admin service/Apache server and all related services will automatically be stopped and restarted.

Procedure

1. Log on to the Microsoft Exchange Server with Administrator rights.
2. Click Control Panel > Add or Remove Programs.
4. Follow the on-screen instructions.
Managing Groups

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

In Worry-Free Business Security, groups are a collection of agents that share the same configuration and run the same tasks. Organize agents into groups in the Security Settings screen so you can simultaneously configure and manage them.

Security Groups Tree and Agents List

In the Security Settings screen, groups appear under the **Security Groups Tree** section on the left side. For ease of management, create groups that represent departments or functions in your company. You can also create special groups. For example, create a group that includes Security Agents on clients that are at a greater risk of infection so you can apply stricter security policies and settings to the group.

When you click a group, the agents that belong to that group display in the **Agents List** to the right.

Agents List Columns

The columns in the Agents List show the following information for each agent:
Tip
Red-shaded cells in the Agents List contain information that requires your attention.

<table>
<thead>
<tr>
<th>COLUMN</th>
<th>INFORMATION SHOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For Security Agents</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Host name of the client where the agent is installed</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the client where the agent is installed</td>
</tr>
<tr>
<td>Online/Offline</td>
<td>• Online: The agent is connected to the Security Server</td>
</tr>
<tr>
<td></td>
<td>• Offline: The agent is disconnected from the Security Server</td>
</tr>
<tr>
<td>Scheduled Scan</td>
<td>Date and time of the last Scheduled Scan</td>
</tr>
<tr>
<td>Manual Scan</td>
<td>Date and time of the last Manual Scan</td>
</tr>
<tr>
<td>Platform</td>
<td>Operating system of the client where the agent is installed</td>
</tr>
<tr>
<td>Architecture</td>
<td>• x64: 64-bit operating system</td>
</tr>
<tr>
<td></td>
<td>• x86: 32-bit operating system</td>
</tr>
<tr>
<td>Scan Method</td>
<td>• Smart: Local and in-the-cloud scans</td>
</tr>
<tr>
<td></td>
<td>• Conventional: Local scans only</td>
</tr>
<tr>
<td></td>
<td>For details, see Scan Methods on page 5-3.</td>
</tr>
<tr>
<td>Virus Engine</td>
<td>Virus Scan Engine version</td>
</tr>
<tr>
<td>Smart Scan Agent Pattern</td>
<td>Smart Scan Agent Pattern version</td>
</tr>
<tr>
<td>COLUMN</td>
<td>INFORMATION SHOWN</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Smart Scan Service     | • **Connected**: The agent is connected to the Smart Scan Service  
|                        | • **Disconnected**: The agent is disconnected from the Smart Scan Service  
|                        | **Note** The Smart Scan Service is hosted on the Security Server. If an agent is disconnected, it means that it cannot connect to the Security Server or the Smart Scan Service is not functional (for example, if the service has been stopped). |
| Virus Pattern          | Virus Pattern version  
|                        | **Note** This column only displays if the scan method is conventional scan.                                                                                                                                               |
| Viruses Detected       | Number of viruses/malware detected                                                                                                                                                                                      |
| Spyware Detected       | Number of spyware/grayware detected                                                                                                                                                                                     |
| Version                | Version of the agent                                                                                                                                                                                                   |
| URLs Violated          | Number of prohibited URLs accessed                                                                                                                                                                                    |
| Spam Detected          | Number of spam email messages                                                                                                                                                                                          |
| POP3 Scan              | • **Enabled**  
|                        | • **Disabled**                                                                                                                                                                                                         |
|                        | **For Messaging Security Agents (Advanced only)**                                                                                                                                                                       |
| Name                   | Host name of the client where the agent is installed                                                                                                                                                                   |
| IP Address             | IP address of the client where the agent is installed                                                                                                                                                                  |
Tasks for Groups and Agents

Run tasks on a group or one or several agents.

Running a task involves two steps:

1. Select a target.
2. Click the button for the task.

The following table lists the tasks that you can perform.
<table>
<thead>
<tr>
<th>Task</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure</td>
<td>One Security Agent group (desktop or server)</td>
<td>Configure the following basic security settings for all Security Agents belonging to the selected group:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Scan method. See Configuring Scan Methods on page 5-5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Antivirus/Anti-spyware. See Configuring Real-time Scan for Security Agents on page 5-7.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Firewall. See Configuring the Firewall on page 5-10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Reputation. See Configuring Web Reputation for Security Agents on page 5-16.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• URL Filtering. See Configuring URL Filtering on page 5-17.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Behavior Monitoring. See Configuring Behavior Monitoring on page 5-19.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device Control. See Configuring Device Control on page 5-23.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User Tools (desktop groups only). See Configuring User Tools on page 5-25.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Client Privileges. See Configuring Client Privileges on page 5-26.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quarantine. See Configuring the Quarantine Directory on page 5-30.</td>
</tr>
</tbody>
</table>
### Configure One Messaging Security Agent (Advanced only)

Configure the following basic security settings for the selected Messaging Security Agent:

- **Antivirus.** See [Configuring Real-time Scan for Messaging Security Agents on page 6-5](#).
- **Anti-spam.** See [Configuring Email Reputation on page 6-7](#) and [Configuring Content Scanning on page 6-9](#).
- **Content Filtering.** See [Managing Content Filtering Rules on page 6-15](#).
- **Attachment Blocking.** See [Configuring Attachment Blocking on page 6-43](#).
- **Web Reputation.** See [Configuring Web Reputation for Messaging Security Agents on page 6-47](#).
- **Quarantine.** See [Querying Quarantine Directories on page 6-50](#), [Maintaining Quarantine Directories on page 6-53](#), and [Configuring Quarantine Directories on page 6-54](#).
- **Operations.** See [Configuring Notification Settings for Messaging Security Agents on page 6-56](#), [Configuring Spam Maintenance on page 6-57](#), and [Generating System Debugger Reports on page 6-61](#).

### Replicate Settings

The settings of the selected group will be applied by another group of the same type (desktop group or server group).

For details, see [Replicating Settings on page 4-17](#).
<table>
<thead>
<tr>
<th>TASK</th>
<th>TARGET</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>One Security Agent group (desktop or server)</td>
<td>Import the settings of a source group to the selected target group. Before importing, be sure that you have exported the settings of the source group to a file. For details, see <em>Importing and Exporting the Settings of Security Agent Groups on page 4-19</em>.</td>
</tr>
<tr>
<td>Export</td>
<td>One Security Agent group (desktop or server)</td>
<td>Export the settings of the selected target group to a file. Perform this task to back up the settings or to import them to another group. For details, see <em>Importing and Exporting the Settings of Security Agent Groups on page 4-19</em>.</td>
</tr>
<tr>
<td>Add Group</td>
<td>Security Groups Tree (👨‍💻)</td>
<td>Add a new Security Agent group (desktop or server group). For details, see <em>Adding Groups on page 4-10</em>.</td>
</tr>
</tbody>
</table>
| Add         | Security Groups Tree (👨‍💻)               | Install one of the following:  
  - **Security Agent** to a client (desktop or server)  
  - **Messaging Security Agent** to a Microsoft Exchange Server (Advanced only)  
For details, see *Adding Agents to Groups on page 4-11*. |
### Description

#### Remove

**Target:** One Security Agent group (desktop or server)

Remove the selected group from the **Security Groups Tree**.

Be sure that the group does not have any agents or the group will not be deleted.

For details, see *Removing Agents on page 3-37*.

#### Remove

**Target:** One or several Security Agents belonging to a group

You have two options:
- Remove the selected Security Agents from their group.
- Uninstall the selected Security Agents from their clients and remove them from their group.

For details, see *Removing Agents on page 3-37*.

#### One Messaging Security Agent (Advanced only)

**Target:** You have two options:
- Remove the selected Messaging Security Agent and its group.
- Uninstall the selected Messaging Security Agents from the Microsoft Exchange server and remove its group.

For details, see *Removing Agents on page 3-37*.

#### Move

**Target:** One or several Security Agents belonging to a group

Move the selected Security Agents to another group or to another Security Server.

For details, see *Moving Agents on page 4-12*. 

---

<table>
<thead>
<tr>
<th>Task</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove</td>
<td>One Security Agent group (desktop or server)</td>
<td>Remove the selected group from the <strong>Security Groups Tree</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Be sure that the group does not have any agents or the group will not be deleted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For details, see <em>Removing Agents on page 3-37</em>.</td>
</tr>
<tr>
<td></td>
<td>One or several Security Agents belonging to a group</td>
<td>You have two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remove the selected Security Agents from their group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Uninstall the selected Security Agents from their clients and remove them from their group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For details, see <em>Removing Agents on page 3-37</em>.</td>
</tr>
<tr>
<td></td>
<td>One Messaging Security Agent (Advanced only)</td>
<td>You have two options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remove the selected Messaging Security Agent and its group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Uninstall the selected Messaging Security Agents from the Microsoft Exchange server and remove its group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For details, see <em>Removing Agents on page 3-37</em>.</td>
</tr>
<tr>
<td>Move</td>
<td>One or several Security Agents belonging to a group</td>
<td>Move the selected Security Agents to another group or to another Security Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For details, see <em>Moving Agents on page 4-12</em>.</td>
</tr>
</tbody>
</table>
## Adding Groups

Add a server group or desktop group, which can contain one or several Security Agents.

It is not possible to add a group containing Messaging Security Agents. After a Messaging Security Agent is installed and reports to the Security Server, it will automatically be its own group in the Security Groups Tree.

### Procedure

1. Navigate to Security Settings.
2. Click Add Group.
   
   A new screen appears.
3. Select a group type.
   - Desktops
   - Servers
4. Type a name for the group.
5. To apply the settings of an existing group to the group you are adding, click **Import settings from group** and then select the group. Only groups for the selected group type will be shown.

6. Click **Save**.

---

## Adding Agents to Groups

After an agent is installed and reports to the Security Server, the server adds it to a group.

- Security Agents installed on server platforms, such as Windows Server 2003 and Windows Server 2008, are added to the **Servers (default)** group.
- Security Agents installed on desktop platforms, such as Windows XP, Windows Vista, and Windows 7, are added to the **Desktops (default)** group.

---

**Note**

You can assign Security Agents to other groups by moving them. For details, see *Moving Agents on page 4-12*.

---

- Each Messaging Security Agent (Advanced only) is its own group. It is not possible to organize several Messaging Security Agents into one group.

If the number of agents reflected on the Security Groups Tree is incorrect, it is possible that agents may have been removed without the server being notified (for example, if client-server communication was lost while removing the agent). This causes the server to retain agent information in its database and show the agent as offline on the web console. When you reinstall the agent, the server creates a new record in the database and treats the agent as new, causing duplicate agents to appear on the Security Groups Tree. To check for duplicate agent records, use the Agent Connection Verification feature in **Preferences > Global Settings > System**.

## Installing Security Agents

See the following topics:

- **Security Agent Installation Requirements on page 3-2**
• Security Agent Installation Considerations on page 3-2
• Security Agent Installation Methods on page 3-8
  • Installing from the Internal Web Page on page 3-10
  • Installing with Login Script Setup on page 3-13
  • Installing with Client Packager on page 3-14
  • Installing with Remote Install on page 3-18
  • Installing with Vulnerability Scanner on page 3-21
  • Installing with Email Notification on page 3-31
• Performing Post-installation Tasks on Security Agents on page 3-33

Installing Messaging Security Agents (Advanced only)

See the following topics:

• Messaging Security Agent Installation Requirements on page 3-35
• Installing the Messaging Security Agent (Advanced only) on page 3-35

Moving Agents

There are several ways to move agents.
### Moving Security Agents Between Groups

#### Procedure

1. Navigate to **Security Settings**.
2. Select a desktop or server group.
3. Select the agents to move.

<table>
<thead>
<tr>
<th>Agent to Move</th>
<th>Details</th>
<th>How to Move Agents</th>
</tr>
</thead>
</table>
| Security Agent | Move Security Agents between groups. After moving, agents inherit the settings of their new group. | Use the web console to move one or several agents. See *Moving Security Agents Between Groups on page 4-13.*

If you have at least two Security Servers, move Security Agents between servers. After moving, an agent will be grouped under the **Desktops (default)** or **Servers (default)** group in the other Security Server, depending on the operating system of the client. The agent inherits the settings of its new group.

- Use the web console to move one or several agents. See *Moving Agents Between Security Servers Using the Web Console on page 4-14.*
- Run the Client Mover tool on a client to move the agent installed on that client. See *Moving a Security Agent Between Security Servers Using Client Mover on page 4-15.*

| Messaging Security Agent (Advanced only) | If you have at least two Security Servers, move Messaging Security Agents between servers. After moving, an agent will be its own group in the other Security Server and will retain its settings. | Use the web console to move one agent at a time. See *Moving Agents Between Security Servers Using the Web Console on page 4-14.* |
Tip
To select multiple, adjacent Security Agents, click the first agent in the range, hold down the SHIFT key, and then click the last agent in the range. To select a range of non-contiguous agents, click the first agent in the range, hold down the CTRL key, and then click the agents you want to select.

4. Drag-and-drop the agents to their new group.

Moving Agents Between Security Servers Using the Web Console

Before you begin

When moving an agent between Security Servers:

• If an agent running an earlier version moves to a Security Server running the current version, the agent will be upgraded automatically.

• Do not move an agent running the current version to a Security Server running a previous version because the agent will become unmanaged (the agent will unregister from its previous server but will fail to register to its new server, therefore, it will not appear in either web console). The agent will keep its current version and will not downgrade.

• The Security Servers must be of the same language version.

• Record the host name and listening port of the Security Server to which an agent will move. The host name and listening port are found on the Security Server’s Security Settings screen, above the Tasks panel.

Procedure

1. On the web console of the Security Server that currently manages the agents, navigate to Security Settings.

2. To move Security Agents, select a group and then select the agents. To move a Messaging Security Agent, select it.
Managing Groups

Tip
To select multiple, adjacent Security Agents, click the first agent in the range, hold down the SHIFT key, and then click the last agent in the range. To select a range of non-contiguous agents, click the first agent in the range, hold down the CTRL key, and then click the agents you want to select.

3. Click Move.

A new screen appears.

4. Type the host name and listening port of the Security Server to which agents will move.

5. Click Move.

6. To check if the agents now report to the other Security Server, open that server’s web console and locate the agents in the Security Groups Tree.

Note
If the agents do not appear in the Security Groups Tree, restart the server’s Master Service (ofservice.exe).

Moving a Security Agent Between Security Servers Using Client Mover

Before you begin
When moving an agent between Security Servers:

• If an agent running an earlier version moves to a Security Server running the current version, the agent will be upgraded automatically.

• Do not move an agent running the current version to a Security Server running a previous version because the agent will become unmanaged (the agent will unregister from its previous server but will fail to register to its new server, therefore, it will not appear in either web console). The agent will keep its current version and will not downgrade.
• The Security Servers must be of the same language version.
• Record the host name and listening port of the Security Server to which an agent will move. The host name and listening port are found on the Security Server’s Security Settings screen, above the Tasks panel.
• Log on to the client using an administrator account.

Procedure
1. On the Security Server that currently manages the agent, go to `<Server installation folder>\PCCSRV\Admin\Utility\IpXfer`.
2. Copy IpXfer.exe to the client where the Security Agent is installed.
3. On the client, open a command prompt.
4. Type `cd` and the path to the folder where you copied the executable file. For example: `cd C:\Test`
5. Run Client Mover using the following syntax:

   `<executable file name> -s <server name> -p <server listening port> -m 1 -c <client listening port>`

<table>
<thead>
<tr>
<th><strong>Parameter</strong></th>
<th><strong>Explanation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;executable file name&gt;</code></td>
<td>IpXfer.exe</td>
</tr>
<tr>
<td><code>&lt;server name&gt;</code></td>
<td>The name of the destination WFBS server (the server to which the agent will transfer)</td>
</tr>
<tr>
<td><code>&lt;server listening port&gt;</code></td>
<td>The listening port (or trusted port) of the destination Security Server.</td>
</tr>
<tr>
<td><code>1</code></td>
<td>The HTTP-based server (you must use the number “1” after “-m”)</td>
</tr>
<tr>
<td><code>&lt;client listening port&gt;</code></td>
<td>The port number used by the Security Agent to communicate with the server</td>
</tr>
</tbody>
</table>
Example:

```
ipXfer.exe -s Server01 -p 8080 -m 1 -c 21112
```

6. To check if the Security Agent now reports to the other Security Server, open that server’s web console and locate the agent in the Security Groups Tree.

---

**Note**

If the agent does not appear in the Security Groups Tree, restart the server’s Master Service (`ofservice.exe`).

---

**Replicating Settings**

Replicate settings between Security Agent groups or between Messaging Security Agents (Advanced only).

**Replicating Security Agent Group Settings**

Use this feature to apply the settings of a particular desktop or server group to another group of the same type. It is not possible to replicate the settings of a server group to a desktop group, and vice versa.

If there is only one group for a particular group type, this feature will be disabled.

**Procedure**

1. Navigate to Security Settings.
2. Select a desktop or server group.
3. Click Replicate Settings.
   
   A new screen appears.
4. Select the target groups that will inherit the settings.
5. Click Apply.

Replicating Messaging Security Agent Settings (Advanced only)

You can only replicate settings between Messaging Security Agents if they share the same domain.

Procedure
1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.
3. Click **Replicate Settings**.
   A new screen appears.
4. Select the Messaging Security Agent that will inherit the settings.
5. Click **Apply**.
6. If replication was unsuccessful:
   a. Start Registry Editor (regedit).
   b. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`.
   c. Right click **winreg > Permissions**.
   d. Add **Smex Admin Group** of target domain, and enable **Allow Read**.
Importing and Exporting the Settings of Security Agent Groups

Export the settings of a desktop or server group to a .dat file to back up the settings. You can also use the .dat file to import the settings to another group.

**Note**

You can import/export settings between desktop and server groups. Settings are not dependent on group type. You can also use the Replicate Settings feature, although this feature is dependent on the group type. For details about the Replicate Settings feature, see Replicating Settings on page 4-17.

**Settings that can be Imported and Exported**

The settings that can be imported and exported depend on whether you chose the Security Groups Tree icon ( ) or a particular desktop/server group.
<table>
<thead>
<tr>
<th>Selection</th>
<th>Screen That Contains the Settings</th>
<th>Settings That Can Be Exported/Imported</th>
</tr>
</thead>
</table>
| Security Groups Tree icon (雯)  | Security Settings (Security Settings > Configure) | The following settings for the Servers (Default) and Desktops (Default) groups:  
• Scan Method  
• Firewall  
• Web Reputation  
• URL Filtering  
• Behavior Monitoring  
• Trusted Program  
• User Tools (Available only on desktop groups)  
• Client Privileges  
• Quarantine  
• Device Control |
| Scheduled Update (Updates > Scheduled) | Components selected and schedule in the Scheduled Update screen |
| Scheduled Reports (Reports > Scheduled Reports) | All settings |
| Report Maintenance (Reports > Maintenance) | All settings |
| Notifications (Preferences > Notifications) | All settings |
| Global Settings (Preferences > Global Settings) | All settings on the following tabs:  
• Proxy  
• SMTP  
• Desktop/Server  
• System |
### Managing Groups

<table>
<thead>
<tr>
<th>Selection</th>
<th>Screen That Contains the Settings</th>
<th>Settings That Can Be Exported/Imported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop group (Desktop) or Server group (Server)</td>
<td>Security Settings (<a href="#">Security Settings &gt; Configure</a>)</td>
<td>• Antivirus/Anti-spyware Real-time Scan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Firewall</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• URL Filtering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Behavior Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Trusted Program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User Tools (<a href="#">Available only on desktop groups</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Client Privileges</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quarantine</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device Control</td>
</tr>
<tr>
<td>Manual Scan screen (<a href="#">Scans &gt; Manual Scan</a>)</td>
<td>All settings</td>
<td></td>
</tr>
<tr>
<td>Scheduled Scan screen (<a href="#">Scans &gt; Scheduled Scan</a>)</td>
<td>All settings</td>
<td></td>
</tr>
</tbody>
</table>

### Exporting Settings

**Procedure**

1. **Navigate to Security Settings.**
2. **Select the Security Groups Tree or a desktop/server group.**
3. **Click Export.**
   
   A new screen appears.
4. **If you selected the Security Groups Tree, select the settings to export.**
5. **Click Export.**
A dialog box appears.

6. Click **Save**, browse to your preferred location, and then click **Save**.

---

**Importing Settings**

---

**Procedure**

1. Navigate to **Security Settings**.

2. Select the Security Groups Tree or a desktop/server group.

3. Click **Import**.
   
   A new screen appears.

4. Click **Browse**, find the file, and then click **Import**.
Chapter 5

Managing Basic Security Settings for Security Agents

This chapter explains how to configure basic security settings for Security Agents.
## Summary of Basic Security Settings for Security Agents

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Method</td>
<td>Configure whether Smart Scan is enabled or disabled.</td>
<td>Enabled or Disabled is chosen during WFBS installation.</td>
</tr>
<tr>
<td>Antivirus/Anti-spyware</td>
<td>Configure Real-time Scan, antivirus, and anti-spyware options</td>
<td>Enabled (Real-time Scan)</td>
</tr>
<tr>
<td>Firewall</td>
<td>Configure Firewall options</td>
<td>Disabled</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>Configure In Office and Out of Office Web Reputation options</td>
<td>In Office: Enabled, Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Out of Office: Enabled, Medium</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>URL filtering blocks websites that violate configured policies.</td>
<td>Enabled, Low</td>
</tr>
<tr>
<td>Behavior Monitoring</td>
<td>Configure Behavior Monitoring options</td>
<td>Enabled for Desktop Groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled for Server Groups</td>
</tr>
<tr>
<td>Trusted Program</td>
<td>Specify which programs do not need to be monitored for suspicious behavior</td>
<td>N/A</td>
</tr>
<tr>
<td>Device Control</td>
<td>Configure Autorun and USB and network access</td>
<td>Disabled</td>
</tr>
<tr>
<td>User Tools</td>
<td>Configure Wi-Fi Advisor and Trend Micro Anti-spam Toolbar</td>
<td>Disabled: Wi-Fi Advisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled: Anti-spam Toolbar in supported email clients</td>
</tr>
</tbody>
</table>
### Scan Methods

Security Agents can use one of two scan methods when scanning for security threats.

- **Smart scan**: Security Agents that use smart scan are referred to as *smart scan agents* in this document. Smart scan agents benefit from local scans and in-the-cloud queries provided by File Reputation Services.

- **Conventional scan**: Security Agents that do not use smart scan are referred to as *conventional scan agents*. A conventional scan agent stores all components on the client and scans all files locally.

The following table provides a comparison between the two scan methods:

**Table 5-2. Conventional Scan and Smart Scan Compared**

<table>
<thead>
<tr>
<th>Basis of Comparison</th>
<th>Conventional Scan</th>
<th>Smart Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Available in this and all earlier WFBS versions</td>
<td>Available starting in WFBS 6.0</td>
</tr>
<tr>
<td><strong>Basis of Comparison</strong></td>
<td><strong>Conventional Scan</strong></td>
<td><strong>Smart Scan</strong></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Scanning behavior       | The conventional scan agent performs scanning on the client. | • The smart scan agent performs scanning on the client.  
  • If the agent cannot determine the risk of the file during the scan, the agent verifies the risk by sending a scan query to the Scan Server (for agents connected to the Security Server) or the Trend Micro Smart Protection Network (for agents disconnected from the Security Server). |
|                         |                       | Note: The Scan Server is a service running on the Security Server. For details, see *Scan Server* on page 2-2.  
  • The agent "caches" the scan query result to improve the scan performance. |
| Components in use and updated | All Security Agent components available on the update source, except the Smart Scan Agent Pattern | All components available on the update source, except the Virus Pattern |
| Typical update source | Security Server | Security Server |
Configuring Scan Methods

Before you begin

When you installed the Security Server, you are given the option to enable smart scan. If you enabled the option, the default scan method is smart scan, which means that all Security Agents will use smart scan. Otherwise, the default is conventional scan. You can switch agents between these scan methods according to your current requirements. For example:

• If agents currently use conventional scan and scanning takes a considerable amount of time to complete, you can switch to smart scan, which was designed to be faster and more efficient. Another instance you might switch to smart scan is when disk space on the agent is running low because smart scan agents download smaller pattern sizes and therefore require less disk space.

Before switching to smart scan, navigate to Preferences > Global Settings > Desktop/Servers tab and go to the General Scan Settings section. Be sure that the Disable Smart Scan Service option has been disabled.

• Switch agents to conventional scan if you notice a drop in performance in the Security Server, which may signal that it is unable to handle all scan queries from agents in a timely manner.

The following table lists some considerations when switching scan methods:

**Table 5-3. Considerations When Switching Between Scan Methods**

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Server connection</td>
<td>Ensure that Security Agents can connect to the Security Server. Only online agents will be notified to switch to a different scan method. Offline agents get notified when they become online. Also verify that the Security Server has the latest components because agents need to download new components from the Security Server, namely, Smart Scan Agent Pattern for agents that will switch to smart scan and Virus Pattern for agents that will switch to conventional scan.</td>
</tr>
</tbody>
</table>
### Consideration and Details

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Security Agents to switch</td>
<td>Switching a relatively small number of Security Agents at a time allows efficient use of Security Server resources. The Security Server can perform other critical tasks while agents change their scan methods.</td>
</tr>
<tr>
<td>Timing</td>
<td>When switching Security Agents for the first time, agents need to download the full version of the Smart Scan Agent Pattern (for agents that will switch to smart scan) or Virus Pattern (for agents that will switch to conventional scan). Consider switching during off-peak hours to ensure the download process finishes within a short amount of time. Also temporarily disable &quot;Update Now&quot; on agents to prevent user-initiated updates and re-enable it after the agents have switched scan methods.</td>
</tr>
<tr>
<td>IPv6 support</td>
<td>A pure IPv6 smart scan agent that is offline cannot send queries directly to the Trend Micro Smart Protection Network. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the smart scan agent to send queries.</td>
</tr>
</tbody>
</table>

### Note

Subsequently, agents will download smaller, incremental versions of the Smart Scan Agent Pattern or Virus Pattern as long as they are updated frequently.

### Procedure

1. Navigate to Security Settings.
2. Select a desktop or server group.
3. Click Configure.
   
   A new screen appears.
4. Select your preferred scan method.
5. Click Save.

---

**Real-time Scan for Security Agents**

Real-time Scan is a persistent and ongoing scan. Each time a file is opened, downloaded, copied, or modified, Real-time Scan in the Security Agent scans the file for threats.

**Configuring Real-time Scan for Security Agents**

**Procedure**

1. Navigate to Security Settings.
2. Select a desktop or server group.
3. Click Configure.
   A new screen appears.
4. Click Antivirus/Anti-spyware.
   A new screen appears.
5. Select Enable real-time Antivirus/Anti-spyware.
6. Configure scan settings. For details, see Scan Targets and Actions for Security Agents on page 7-8:

   **Note**
   If you grant users the privilege to configure their own scan settings, the user-configured settings will be used during the scan.

7. Click Save.
Firewall

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

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

---

**Tip**

Trend Micro recommends uninstalling other software-based firewalls before deploying and enabling the Trend Micro firewall.

---

**Default Firewall Simple Mode Settings**

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

---

**Note**

By default, WFBS disables the firewall on all new groups and Security Agents.

---

**Table 5-4. Default Firewall Settings**

<table>
<thead>
<tr>
<th>Settings</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Inbound and outbound traffic allowed, only network viruses blocked.</td>
</tr>
<tr>
<td>Intrusion Detection System</td>
<td>Disabled</td>
</tr>
<tr>
<td>Alert Message (send)</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
### Table 5-5. Default Firewall Exceptions

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

### Table 5-6. Default Firewall Settings According to Location

<table>
<thead>
<tr>
<th>Location</th>
<th>Firewall Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Office</td>
<td>Off</td>
</tr>
<tr>
<td>Out of Office</td>
<td>Off</td>
</tr>
</tbody>
</table>

### Traffic Filtering

The firewall filters all incoming and outgoing traffic, providing the ability to block certain types of traffic based on the following criteria:

- Direction (inbound/outbound)
- Protocol (TCP/UDP/ICMP/ICMPv6)
- Destination ports
- Destination computer

**Scanning for Network Viruses**

The firewall also examines each packet for network viruses.

**Stateful Inspection**

The firewall is a stateful inspection firewall; it monitors all connections to the client and remembers all connection states. It can identify specific conditions in any connection, predict what actions should follow, and detect disruptions in a normal connection. Therefore, effective use of the firewall not only involves creating profiles and policies, but also analyzing connections and filtering packets that pass through the firewall.

**Common Firewall Driver**

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

**Configuring the Firewall**

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. For details about Location Awareness, see *Configuring Desktop/Server Settings on page 11-5*.

Trend Micro disables the firewall by default.

**Procedure**

1. Navigate to **Security Settings**.
2. Select a desktop or server group.
3. Click **Configure**.
   
   A new screen appears.
4. Click **Firewall > In Office** or **Firewall > Out of Office**.

   A new screen appears.

5. Select **Enable Firewall**.

6. Select from the following:
   - **Simple Mode**: Enables firewall with default settings. For details, see *Default Firewall Simple Mode Settings on page 5-8*.
   - **Advanced Mode**: Enables firewall with custom settings.

7. If you selected **Advanced Mode**, update the following options as required:
   - **Security Level**: The security level controls the traffic rules to be enforced for ports not in the exception list.
     - **High**: blocks all incoming and outgoing traffic except any traffic allowed in the exception list.
     - **Medium**: blocks all incoming traffic and allows all outgoing traffic except any traffic allowed and blocked in the exception list.
     - **Low**: allows all incoming and outgoing traffic except any traffic blocked in the exception list. This is the default setting for the Simple mode.
   - **Settings**
     - **Enable Intrusion Detection System**: Intrusion Detection System identifies patterns in network packets that may indicate an attack. See *Intrusion Detection System on page D-4*.
     - **Enable Alert Messages**: When WFBS detects a violation, the client is notified.
     - **Exceptions**: Ports in the exception list will not be blocked. See *Working with Firewall Exceptions on page 5-12*.

8. Click **Save**.

   The changes take effect immediately.
Working with Firewall Exceptions

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

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

Procedure

1. Navigate to Security Settings.
2. Select a desktop or server group.
3. Click Configure.
   
   A new screen appears.
4. Click Firewall > In Office or Firewall > Out of Office.
   
   A new screen appears.
5. Select Enable Firewall.
6. Select Advanced Mode.
7. To add an exception:
   a. Click Add.
      
      A new screen appears.
   b. Type the name for the exception.
   c. Next to Action, click one of the following:
      
      • Allow all network traffic
      • Deny all network traffic
d. Next to **Direction**, click **Inbound** or **Outbound** to select the type of traffic to which to apply the exception settings.

e. Select the type of network protocol from the Protocol list:
   - **All**
   - **TCP/UDP** (default)
   - **TCP**
   - **UDP**
   - **ICMP**
   - **ICMPv6**

f. Click one of the following to specify client ports:
   - **All ports** (default)
   - **Range**: type a range of ports
   - **Specified ports**: specify individual ports. Use a comma "," to separate port numbers.

g. Under **Machines**, select client IP addresses to include in the exception. For example, if you select **Deny all network traffic (Inbound and Outbound)** and type the IP address for a client on the network, then any client that has this exception in its policy will not be able to send or receive data to or from that IP address. Click one of the following:
   - **All IP addresses** (default)
   - **Single IP**: Type an IPv4 or IPv6 address, or a host name. To resolve the client host name to an IP address, click **Resolve**.
   - **IP range (for IPv4 or IPv6)**: Type either two IPv4 or two IPv6 addresses in the **From** and **To** fields. It is not possible to type an IPv6 address in one field and an IPv4 address in the other field.
   - **IP range (for IPv6)**: Type an IPv6 address prefix and length.

h. Click **Save**.
8. To edit an exception, click **Edit** and then modify the settings in the screen that displays.

9. To move an exception up or down the list, select the exception and then click **Move Up** or **Move Down** until it is in your preferred position.

10. To remove an exception, select the exception and then click **Remove**.

---

**Disabling the Firewall on a Group of Agents**

**Procedure**

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure**.

   A new screen appears.

4. Click **Firewall > In Office** or **Firewall > Out of Office**.

   A new screen appears.

5. Select **Disable Firewall**.

6. Click **Save**.

---

**Disabling the Firewall on All Agents**

**Procedure**

1. Navigate to **Preferences > Global Settings > Desktop/Server** tab.

2. Under **Firewall Settings**, select **Disable Firewall and uninstall drivers**.

3. Click **Save**.
Web Reputation

Web Reputation helps prevent access to URLs on the web or embedded in email messages that pose security risks. Web Reputation checks the URL’s reputation against the Trend Micro web reputation servers and then correlates the reputation with the specific web reputation policy enforced on the client. Depending on the policy in use:

- The Security Agent will block or allow access to the website.
- The Messaging Security Agent (Advanced only) will quarantine, delete, or tag the email message containing malicious URLs, or allow the message to be sent if the URLs are safe.

Web Reputation provides both email notification to the administrator and online notification to the user for detections.

For Security Agents, configure a different level of security based on the location (In Office/Out of Office) of the client.

If Web Reputation blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list.

Tip
To save network bandwidth, Trend Micro recommends adding the enterprise internal websites to the Web reputation approved URL list.

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 if its score falls within a defined threshold, and safe if its score exceeds the threshold.

A Security Agent has three security levels that determine whether it will allow or block access to a URL.

- **High**: Blocks pages that are:
  - **Dangerous**: Verified to be fraudulent or known sources of threats
Highly suspicious: Suspected to be fraudulent or possible sources of threats

Suspicious: Associated with spam or possibly compromised

Untested: While Trend Micro actively tests web pages for safety, users may encounter untested pages when visiting new or less popular websites. Blocking access to untested pages can improve safety but can also prevent access to safe pages.

Medium: Blocks pages that are:

• Dangerous: Verified to be fraudulent or known sources of threats
• Highly suspicious: Suspected to be fraudulent or possible sources of threats

Low: Blocks pages that are:

• Dangerous: Verified to be fraudulent or known sources of threats

Configuring Web Reputation for Security Agents

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

Note

(Standard Only) Configure the Web Reputation settings for In Office and Out of Office. If Location Awareness is disabled, In Office settings will be used for Out of Office connections. For details about Location Awareness, see Configuring Desktop/Server Settings on page 11-5.

Procedure

1. Navigate to Security Settings.
2. Select a desktop or server group.
3. Click Configure.
   A new screen appears.
4. Click Web Reputation > In Office or Web Reputation > Out of Office.
A new screen appears.

5. Update the following as required:
   - **Enable Web Reputation**
   - Security Level: **High**, **Medium**, or **Low**
   - Approved URL(s)
     - **URLs to approve**: Separate multiple URLs with semicolons (;). Click **Add**.
     - **Approved URL list**: URLs in this list will not be blocked. To delete an entry, click the corresponding trash can icon.

6. **Click Save**.

**URL Filtering**

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

**Configuring URL Filtering**

You can select specific types of websites to block during different times of the day by selecting **Custom**.
Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure**.

   A new screen appears.

4. Click **URL Filtering**.

   A new screen appears.

5. 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.
   - **Filter Rules**: Select entire categories or sub-categories to block.
   - **Business Hours**: Any days or hours that are not defined under Business Hours are considered Leisure hours.
   - **URL Filtering**
     - **URLs to approve**: Separate multiple URLs with semicolons (;). Click **Add**.
     - **Approved URL list**: URLs in this list will not be blocked. To delete an entry, click the corresponding trash can icon.
     - **URLs to block**: Separate multiple URLs with semicolons (;). Click **Add**.
• **Blocked URL list:** URLs in this list will be blocked. To delete an entry, click the corresponding trash can icon.

---

**Note**

Use wildcards with caution as they may allow or block large sets of URLs.

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

The approved list takes precedence over the blocked list. When a URL matches an entry in the approved list, the URL is automatically allowed and is not checked against the blocked list.

6. Click **Save**.

---

**Behavior Monitoring**

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

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

**Configuring Behavior Monitoring**

**Procedure**

1. Navigate to **Security Settings**.
2. Select a desktop or server group.
3. Click **Configure**.
A new screen appears.

4. Click **Behavior Monitoring**.

A new screen appears.

5. Update the following as required:

   - **Enable Behavior Monitoring**

   **Note**

   To allow users to customize their own Behavior Monitoring settings, go to **Security Settings > [group] > Configure > Client Privileges > Behavior Monitoring** and select **Allow users to modify Behavior Monitoring settings**.

   - **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

   **Note**

   All Intuit executable files have a digital signature and updates to these files will not be blocked. If 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. Other programs can be allowed to update Intuit files. To do this, add the required program to the Behavior Monitoring Exception List on the Agent. Remember to remove the program from the exception list after the update.
• **Enable Malware Behavior Blocking**: A group of technologies based on rule sets that attempt to identify certain suspicious behaviors that are common amongst malware or Fake Anti-Virus. Examples of such behaviors may include sudden and unexplainable new running services, changes to the firewall, system file modifications, etc.

• **Exceptions**: Exceptions include an Approved Program List and a Blocked Program List. Programs in the Approved Programs List can be started even if they violate a monitored change, while programs in the Blocked Program List can never be started.

• **Enter Program Full Path**: Type the full Windows or UNC path of the program. Separate multiple entries with semicolons. Click **Add to Approved List** or **Add to Blocked List**. Use environment variables to specify paths, if required.

<table>
<thead>
<tr>
<th><strong>ENVIRONMENT VARIABLE</strong></th>
<th><strong>POINTS TO THE...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>$windir$</td>
<td>Windows folder</td>
</tr>
<tr>
<td>$rootdir$</td>
<td>root folder</td>
</tr>
<tr>
<td>$tempdir$</td>
<td>Windows temporary folder</td>
</tr>
<tr>
<td>$programdir$</td>
<td>Program Files folder</td>
</tr>
</tbody>
</table>

• **Approved Program List**: Programs (maximum of 100) in this list can be started. Click the corresponding icon to delete an entry

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

6. Click **Save**.

---

**Trusted Program**

Programs listed in the Trusted Program List will not be monitored for suspicious file access activities.
Configuring Trusted Program

Procedure

1. Navigate to Security Settings.

2. Select a desktop or server group.

3. Click Configure.

   A new screen appears.

4. Click Trusted Program.

   A new screen appears.

5. To exclude a program from suspicious file access activity monitoring, type the full file path, using a specific file path, and click Add to Trusted Program List.

   \<drive_name>:/<path>/<file_name>

   Example 1: C:\Windows\system32\regedit.exe

   Example 2: D:\backup\tool.exe

   This prevents hackers from using program names in the exclusion list but dropped in different file path to be executed.

6. Click Save.

Device Control

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

Procedure

1. Navigate to Security Settings.
2. Select a desktop or server group.
3. Click Configure.
   
   A new screen appears.
4. Click Device Control.
   
   A new screen appears.
5. Update the following as required:
   
   • Enable Device Control
   • Enable USB Autorun Prevention
   • Permissions: Set for both USB devices and network resources.

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Files on the Device</th>
<th>Incoming Files</th>
</tr>
</thead>
</table>
| Full access | Permitted operations: Copy, Move, Open, Save, Delete, Execute | Permitted operations: Save, Move, Copy
|             |                     | This means that a file can be saved, moved, and copied to the device. |
| Modify      | Permitted operations: Copy, Move, Open, Save, Delete
<pre><code>         | Prohibited operations: Execute | Permitted operations: Save, Move, Copy |
</code></pre>
<table>
<thead>
<tr>
<th>Permissions</th>
<th>Files on the Device</th>
<th>Incoming Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read and execute</td>
<td>Permitted operations: Copy, Open, Execute</td>
<td>Prohibited operations: Save, Move, Copy</td>
</tr>
<tr>
<td></td>
<td>Prohibited operations: Save, Move, Delete</td>
<td></td>
</tr>
<tr>
<td>Read</td>
<td>Permitted operations: Copy, Open</td>
<td>Prohibited operations: Save, Move, Copy</td>
</tr>
<tr>
<td></td>
<td>Prohibited operations: Save, Move, Copy, Execute</td>
<td></td>
</tr>
<tr>
<td>No access</td>
<td>Prohibited operations: All operations</td>
<td>Prohibited operations: Save, Move, Copy</td>
</tr>
<tr>
<td></td>
<td>The device and the files it contains are visible to the user (for example, from Windows Explorer).</td>
<td></td>
</tr>
</tbody>
</table>

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

6. Click **Save**.

---

**User Tools**

- **Wi-Fi Advisor:** Determines the safety of a wireless connection by checking the authenticity of access points based on the validity of their SSIDs, authentication methods, and encryption requirements. A pop-up warning will show if a connection is unsafe.
- **Anti-Spam Toolbar**: Filters spam in Microsoft Outlook, gives statistics, and allows you to change certain settings.

- **Case Diagnostic Tool**: Trend Micro Case Diagnostic Tool (CDT) collects necessary debugging information from a customer’s product whenever problems occur. It automatically turns the product's debug status on and off and collects necessary files according to problem categories. Trend Micro uses this information to troubleshoot problems related to the product.

  This tool is available only on the Security Agent console.

### Configuring User Tools

**Procedure**

1. Navigate to **Security Settings**.
2. Select a desktop or server group.
3. Click **Configure**.
   
   A new screen appears.

4. Click **User Tools**.
   
   A new screen appears.

5. 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 anti-spam toolbar in supported mail clients**

6. Click **Save**.

### Client Privileges

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

Configuring Client Privileges

Procedure
1. Navigate to Security Settings.
2. Select a desktop or server group.
3. Click Configure.
   A new screen appears.
4. Click Client Privileges.
   A new screen appears.
5. Update the following as required:

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PRIVILEGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus/Anti-spyware</td>
<td>• Manual Scan settings</td>
</tr>
<tr>
<td></td>
<td>• Scheduled Scan settings</td>
</tr>
<tr>
<td></td>
<td>• Real-time Scan settings</td>
</tr>
<tr>
<td></td>
<td>• Skip Scheduled Scan</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall Settings</td>
</tr>
<tr>
<td>Web Reputation - Continue Browsing</td>
<td>Will show a link that allows users to continue browsing a particular malicious URL until the computer is restarted. Warnings will still show on other malicious URLs.</td>
</tr>
<tr>
<td>URL Filtering - Continue Browsing</td>
<td>Will show a link that allows users to continue browsing a particular restricted URL until the computer is restarted. Warnings will still show on other restricted URLs.</td>
</tr>
<tr>
<td><strong>SECTION</strong></td>
<td><strong>PRIVILEGES</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Behavior</td>
<td>Allow users to modify Behavior Monitoring settings.</td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Trusted Program</td>
<td>Allow users to modify the Trusted Program list.</td>
</tr>
<tr>
<td>Proxy Settings</td>
<td>Allow users to configure proxy settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Disabling this feature will reset the proxy settings to their default.</td>
</tr>
<tr>
<td>Update Privileges</td>
<td>• Allow users to perform manual updates</td>
</tr>
<tr>
<td></td>
<td>• Use Trend Micro ActiveUpdate as a secondary update source</td>
</tr>
<tr>
<td></td>
<td>• Disable hot fix deployment</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Deploying hot fixes, patches, security/critical patches, and service packs to a large number of</td>
</tr>
<tr>
<td></td>
<td>agents simultaneously can significantly increase network traffic. Consider enabling this option on</td>
</tr>
<tr>
<td></td>
<td>several groups so you can stagger the deployment.</td>
</tr>
<tr>
<td></td>
<td>Enabling this option also disables automatic <strong>build upgrades</strong> on agents (for example, from the Beta</td>
</tr>
<tr>
<td></td>
<td>build to the release build of the current product version) but NOT automatic <strong>version upgrades</strong></td>
</tr>
<tr>
<td></td>
<td>(for example, from version 7.x to the current version).</td>
</tr>
<tr>
<td></td>
<td>To disable automatic version upgrades, run the Security Server installation package and choose the</td>
</tr>
<tr>
<td></td>
<td>option for delaying upgrades.</td>
</tr>
<tr>
<td>Client Security</td>
<td>Prevent users or other processes from modifying Trend Micro program files, registries and processes.</td>
</tr>
</tbody>
</table>

6. Click **Save**.
Quarantine Directory

If the action for an infected file is "Quarantine", the Security Agent encrypts the file and temporarily moves it to a quarantine folder located in:

- `<Security Agent installation folder>\quarantine` for agents upgraded from version 6.x or earlier
- `<Security Agent installation folder>\SUSPECT\Backup` for newly installed agents and those upgraded from version 7.x or later

The Security Agent sends the infected file to a central quarantine directory, which you can configure from the web console, in **Security Settings > {Group} > Configure > Quarantine**.

**Default Central Quarantine Directory**

The default central quarantine directory is located on the Security Server. The directory is in URL format and contains the Security Server’s host name or IP address, such as `http://server`. The equivalent absolute path is `<Security Server installation folder>\PCCSRV\Virus`.

- If the server is managing both IPv4 and IPv6 agents, use the host name so that all agents can send quarantined files to the server.
- If the server only has or is identified by its IPv4 address, only pure IPv4 and dual-stack agents can send quarantined files to the server.
- If the server only has or is identified by its IPv6 address, only pure IPv6 and dual-stack agents can send quarantined files to the server.

**Alternative Central Quarantine Directory**

You can specify an alternative central quarantine directory by typing the location in URL, UNC path, or absolute file path format. Security Agents should be able to connect to this directory. For example, the directory should have an IPv6 address if it will receive quarantined files from dual-stack and pure IPv6 agents. Trend Micro recommends designating a dual-stack directory, identifying the directory by its host name, and using UNC path when typing the directory.
Guidelines on Specifying the Central Quarantine Directory

Refer to the following table for guidance on when to use URL, UNC path, or absolute file path:

**Table 5-8. Quarantine Directory**

<table>
<thead>
<tr>
<th>QUARANTINE DIRECTORY</th>
<th>ACCEPTED FORMAT</th>
<th>EXAMPLE</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default directory on the Security Server</td>
<td>URL</td>
<td><code>http:// &lt;server host name or IP&gt;</code></td>
<td>If you keep the default directory, configure maintenance settings for the directory, such as the size of the quarantine folder, in Preferences &gt; Global Settings &gt; System tab &gt; Quarantine Maintenance section.</td>
</tr>
<tr>
<td></td>
<td>UNC path</td>
<td><code>\&lt;server host name or IP&gt;\ ofcscan\Virus</code></td>
<td></td>
</tr>
<tr>
<td>Another directory on the Security Server</td>
<td>UNC path</td>
<td><code>\&lt;server host name or IP&gt;\ D$ \Quarantined Files</code></td>
<td>If you do not want to use the default directory (for example, if it has insufficient disk space), type the UNC path to another directory. If you do this, type the equivalent absolute path in Preferences &gt; Global Settings &gt; System tab &gt; Quarantine Maintenance section to allow maintenance settings to take effect.</td>
</tr>
</tbody>
</table>
### Configuring the Quarantine Directory

<table>
<thead>
<tr>
<th>QUARANTINE DIRECTORY</th>
<th>ACCEPTED FORMAT</th>
<th>EXAMPLE</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>A directory on another Security Server computer (if you have other Security Servers on the network)</td>
<td>URL</td>
<td>http:// &lt;server2 host name or IP&gt;</td>
<td>Ensure that agents can connect to this directory. If you specify an incorrect directory, the agent keeps the quarantined files until a correct quarantine directory is specified. In the server's virus/malware logs, the scan result is &quot;Unable to send the quarantined file to the designated quarantine folder&quot;. If you use UNC path, ensure that the quarantine directory folder is shared to the group &quot;Everyone&quot; and that you assign read and write permission to this group.</td>
</tr>
<tr>
<td>Another computer on the network</td>
<td>UNC path</td>
<td>&lt;server2 host name or IP&gt;\ ofcscan\Virus</td>
<td></td>
</tr>
</tbody>
</table>
| A different directory on the client | Absolute path | C:\temp | Specify an absolute path if:  
- You want quarantined files to reside only in the client.  
- You do not want agents to store the files in the default directory in the client.  
If the path does not exist, the Security Agent automatically creates it. |

#### Procedure

1. Navigate to **Security Settings**.
2. Select a desktop or server group.
3. Click **Configure**.

A new screen appears.
4. Click **Quarantine**.
   
   A new screen appears.

5. Configure the quarantine directory. For details, see *Quarantine Directory on page 5-28*.

6. Click **Save**.
Chapter 6

Managing Basic Security Settings for Messaging Security Agents (Advanced Only)

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 the agent.
Messaging Security Agents

Messaging Security Agents protect Microsoft Exchange servers. The 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
- Detect malicious URLs in email
- Prevent confidential data leaks

Important Information about Messaging Security Agents

- Messaging Security Agents can only be installed on Microsoft Exchange servers.
- The Security Groups Tree in the web console displays all the Messaging Security Agents. Multiple Messaging Security Agents cannot be combined into a group; each Messaging Security Agent must be administered and managed individually.
- WFBS uses the Messaging Security Agent to gather security information from Microsoft Exchange servers. For example, the Messaging Security Agent reports spam detections or completion of component updates to the Security Server. This information displays in the web console. The Security Server also uses this information to generate logs and reports about the security status of your Microsoft Exchange servers.

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.

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

- `ScanMail_Master`
- `ScanMail_RemoteConfig`

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

How the Messaging Security Agent Scans Email Messages

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

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

Default Messaging Security Agent Settings

Consider the options listed in the table to help you optimize your Messaging Security Agent configurations.
**Table 6-1. Trend Micro Default Actions for the Messaging Security Agent**

<table>
<thead>
<tr>
<th>Scan Option</th>
<th>Real-time Scan</th>
<th>Manual and Scheduled Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anti-spam</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam</td>
<td>Quarantine message to user’s spam folder (default, if the Outlook Junk Email or End User Quarantine installed)</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Phish</td>
<td>Delete entire message</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Content filtering</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filter messages that match any condition defined</td>
<td>Quarantine entire message</td>
<td>Replace</td>
</tr>
<tr>
<td>Filter messages that match all conditions defined</td>
<td>Quarantine entire message</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Monitor the message content of particular email accounts</td>
<td>Quarantine entire message</td>
<td>Replace</td>
</tr>
<tr>
<td>Create an exception for particular email accounts</td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td><strong>Attachment blocking</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Replace attachment with text/file</td>
<td>Replace attachment with text/file</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted and Password protected files</td>
<td>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)</td>
<td>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)</td>
</tr>
</tbody>
</table>
Managing Basic Security Settings for Messaging Security Agents (Advanced Only)

Real-Time Scan for Messaging Security Agents

Real-time Scan is a persistent and ongoing scan. Real-time Scan in the Messaging Security Agent (Advanced only) guards all known virus entry points by scanning all incoming messages, SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers.

Configuring Real-time Scan for Messaging Security Agents

Procedure

1. Navigate to Security Settings.
2. Select a Messaging Security Agent.
3. Click Configure.
   A new screen appears.
4. Click Antivirus.
   A new screen appears.
5. Select Enable real-time antivirus.
6. Configure scan settings. For details, see Scan Targets and Actions for Messaging Security Agents on page 7-15.
7. Click **Save**.

Configure who receives notifications when an event occurs. See *Configuring Events for Notifications on page 9-3*.

---

**Anti-Spam**

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

The Messaging Security Agent uses the following components to filter email messages for spam and phishing incidents:

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

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

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

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

---

**Tip**

In addition to using Anti-Spam to screen out spam, you can configure Content Filtering to filter message header, subject, body, and attachment information to filter out spam and other undesirable content.
Users cannot modify the method that the anti-spam engine uses to assign spam scores, but they can adjust the detection levels used by the Messaging Security Agent to decide what is spam and what is not spam.

**Note**

Microsoft Outlook may automatically filter and send messages that the Messaging Security Agent detected as spam to the Junk Mail folder.

### Email Reputation

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

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

- **Standard**: The Standard service uses a database that tracks the reputation of about two billion IP addresses. IP addresses that have been consistently associated with the delivery of spam messages are added to the database and rarely removed.

- **Advanced**: The Advanced service level is a DNS, query-based service like the Standard service. At the core of this service is the standard reputation database, along with the dynamic reputation, real-time database that blocks messages from known and suspected sources of spam.

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

### Configuring Email Reputation

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

**Procedure**

1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.

3. Click **Configure**.
   
   A new screen appears.

4. Click **Anti-spam > Email Reputation**.
   
   A new screen appears.

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

6. Click **Save**.


---

**Note**

Email Reputation is a Web-based service. Administrators can only configure the service level from the web console.

---

**Content Scanning**

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

**Note**

Do not confuse Content Scanning (anti-spam based on signatures and heuristics) with Content Filtering (email scanning and blocking based on categorized keywords). See [Content Filtering on page 6-14](#).

**Configuring Content Scanning**

The Messaging Security Agent detects spam messages in **real time** and takes actions to protect the Microsoft Exchange Servers.

**Procedure**

1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.
3. Click **Configure**.
   
   A new screen appears.
4. Click **Anti-spam > Content Scanning**.
   
   A new screen appears.
5. Select **Enable real-time Anti-Spam**.
6. Select the **Target** tab to select the method and spam detection rate that the Messaging Security Agent uses to screen for spam:
   
   a. Select the detection level, **low**, **medium**, or **high**, from the spam detection rate list. The Messaging Security Agent uses this rate to screen all messages.
      
      • **High**: This is the most rigorous level of spam detection. The Messaging Security Agent monitors all email messages for suspicious files or text, but there is greater chance of false positives. False positives are those
email messages that the Messaging Security Agent filters as spam when they are actually legitimate email messages.

- **Medium**: This is the default and recommended setting. The Messaging Security Agent monitors at a high level of spam detection with a moderate chance of filtering false positives.

- **Low**: This is the most lenient level of spam detection. The Messaging Security Agent will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives. Filtering by spam score.

b. Click **Detect Phishing** to have the Messaging Security Agent screen out Phishing Incidents. For details, see *Phishing Incidents on page 1-12*.

c. Add addresses to your list of Approved Senders and Blocked Senders. For details, see *Approved and Blocked Senders Lists on page 6-11*.

- **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**.

- **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**.

---

**Note**

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

---

7. Click the **Action** tab to set the actions that the Messaging Security Agent takes when it detects a spam message or phishing incident.
For details about actions, see *Scan Targets and Actions for Messaging Security Agents on page 7-15.*

The Messaging Security Agent takes one of the following actions depending on your configuration:

- Quarantine message to server-side spam folder
- Quarantine message to user's spam folder

**Note**
If you choose this action, configure the End User Quarantine. For details, see *Configuring Spam Maintenance on page 6-57.*

- Delete entire message
- Tag and deliver

8. Click **Save.**

**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 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 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.

**General Guidelines**

- 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 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.

- 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).

**Wildcard Matching**

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 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 6-2. Email Address Matches for Wildcards

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Matched Samples</th>
<th>Unmatched Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:john@example.com">john@example.com</a></td>
<td><a href="mailto:john@example.com">john@example.com</a></td>
<td>Any address different from the pattern</td>
</tr>
<tr>
<td>@example.com</td>
<td><a href="mailto:john@example.com">john@example.com</a></td>
<td><a href="mailto:john@ms1.example.com">john@ms1.example.com</a></td>
</tr>
<tr>
<td>*@example.com</td>
<td><a href="mailto:mary@example.com">mary@example.com</a></td>
<td><a href="mailto:john@ms1.example.com.us">john@ms1.example.com.us</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:mary@example.com.us">mary@example.com.us</a></td>
</tr>
<tr>
<td>example.com</td>
<td><a href="mailto:john@example.com">john@example.com</a></td>
<td><a href="mailto:john@example.com.us">john@example.com.us</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:john@ms1.example.com">john@ms1.example.com</a></td>
<td><a href="mailto:mary@ms1.rd.example.com">mary@ms1.rd.example.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:mary@ms1.rd.example.com">mary@ms1.rd.example.com</a></td>
<td><a href="mailto:joe@ms1.example.com">joe@ms1.example.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:mary@example.com">mary@example.com</a></td>
<td></td>
</tr>
<tr>
<td>*.example.com</td>
<td><a href="mailto:john@ms1.example.com">john@ms1.example.com</a></td>
<td><a href="mailto:john@example.com">john@example.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:mary@ms1.rd.example.com">mary@ms1.rd.example.com</a></td>
<td><a href="mailto:john@myexample.com.us">john@myexample.com.us</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="mailto:mary@ms1.example.com.us">mary@ms1.example.com.us</a></td>
</tr>
<tr>
<td>example.com.*</td>
<td><a href="mailto:john@example.com.us">john@example.com.us</a></td>
<td><a href="mailto:john@example.com">john@example.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:john@ms1.example.com.us">john@ms1.example.com.us</a></td>
<td><a href="mailto:mary@ms1.example.com">mary@ms1.example.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:john@ms1.rd.example.com.us">john@ms1.rd.example.com.us</a></td>
<td><a href="mailto:john@myexample.com.us">john@myexample.com.us</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:mary@example.com.us">mary@example.com.us</a></td>
<td></td>
</tr>
<tr>
<td>example.com.*</td>
<td><a href="mailto:john@ms1.example.com.us">john@ms1.example.com.us</a></td>
<td><a href="mailto:john@example.com">john@example.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:john@ms1.rd.example.com.us">john@ms1.rd.example.com.us</a></td>
<td><a href="mailto:john@myexample.com.us">john@myexample.com.us</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:mary@example.com.us">mary@example.com.us</a></td>
<td></td>
</tr>
<tr>
<td><em>.example.com.</em></td>
<td><a href="mailto:john@ms1.example.com.us">john@ms1.example.com.us</a></td>
<td><a href="mailto:john@example.com">john@example.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:john@ms1.rd.example.com.us">john@ms1.rd.example.com.us</a></td>
<td><a href="mailto:john@myexample.com.us">john@myexample.com.us</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:mary@example.com.us">mary@example.com.us</a></td>
<td></td>
</tr>
<tr>
<td>*.example.com</td>
<td>The same as “*.example.com”</td>
<td></td>
</tr>
<tr>
<td>****.example.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

*example.com  *example.com*  example.*.com  @*.example.com

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Matched Samples</th>
<th>Unmatched Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>*example.com</td>
<td>Invalid patterns</td>
<td></td>
</tr>
<tr>
<td>example.com*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>example.*.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>@*.example.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*example.com  example.com*  example.*.com  @*.example.com

**Note**

Do not confuse Content Scanning (anti-spam based on signatures and heuristics) with Content Filtering (email scanning and blocking based on categorized keywords). See *Content Scanning on page 6-8*.

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
Managing Basic Security Settings for Messaging Security Agents (Advanced Only)

Note
By default, content filtering is not enabled.

Managing Content Filtering Rules

The Messaging Security Agent displays all the Content Filtering rules on the Content Filtering screen. Access this screen by navigating to:

- For Real-time Scan:
  Security Settings > {Messaging Security Agent} > Configure > Content Filtering

- For Manual Scan:
  Scans > Manual > {Expand Messaging Security Agent} > Content Filtering

- For Scheduled Scan:
  Scans > Scheduled > {Expand Messaging Security Agent} > Content Filtering

Procedure

1. View summary information about the rules, including:
   - **Rule**: WFBS comes with default rules that filter content according to the following categories: Profanity, Racial Discrimination, Sexual Discrimination, Hoaxes, and Chainmail. These rules are disabled by default. You can modify these rules according to your requirements or delete them. If none of these rules meet your requirements, add your own rules.
   - **Action**: The Messaging Security Agent takes this action when it detects undesirable content.
   - **Priority**: The Messaging Security Agent applies each filter in succession according to the order shown on this page.
   - **Enabled**: A green icon indicates an enabled rule while a red icon indicates a disabled rule.
2. Perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable/Disable Content Filtering</td>
<td>Select or clear <strong>Enable real-time content filtering</strong> on top of the screen.</td>
</tr>
<tr>
<td>Add a rule</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>A new screen opens where you can choose the type of rule to add. For details, see <em>Types of Content Filtering Rules on page 6-18</em>.</td>
</tr>
<tr>
<td>Modify a rule</td>
<td>a. Click the rule name.</td>
</tr>
<tr>
<td></td>
<td>A new screen opens.</td>
</tr>
<tr>
<td></td>
<td>b. The options available in the screen depend on the type of rule.</td>
</tr>
<tr>
<td></td>
<td>To determine the type of rule, check the breadcrumb on top of the</td>
</tr>
<tr>
<td></td>
<td>screen and note the second item in the breadcrumb.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>Content Filtering &gt; <strong>Match Any Condition Rule</strong> &gt; Edit Rule</td>
</tr>
<tr>
<td></td>
<td>For details about rule settings that you can modify, see any of the</td>
</tr>
<tr>
<td></td>
<td>following topics:</td>
</tr>
<tr>
<td></td>
<td>•  <em>Adding a Content Filtering Rule for Any Matching Condition on page 6-22</em></td>
</tr>
<tr>
<td></td>
<td>•  <em>Adding a Content Filtering Rule for All Matching Conditions on page 6-19</em></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This rule type is not available for Manual and Scheduled Content</td>
</tr>
<tr>
<td></td>
<td>Filtering Scans.</td>
</tr>
<tr>
<td></td>
<td>•  <em>Adding a Content Filtering Monitoring Rule on page 6-24</em></td>
</tr>
<tr>
<td></td>
<td>•  <em>Creating Exceptions to Content Filtering Rules on page 6-27</em></td>
</tr>
</tbody>
</table>
Reorder rules

The Messaging Security Agent applies the Content Filtering rules to email messages according to the order shown in the Content Filtering screen. Configure the order in which the rules are applied. The agent 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.

a. Select a check box that corresponds to the rule for which you want to change the order.

b. Click Reorder.

A box appears around the order number for the rule.

c. In the Priority column box, delete the existing order number and type a new one.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Reorder rules | The Messaging Security Agent applies the Content Filtering rules to email messages according to the order shown in the Content Filtering screen. Configure the order in which the rules are applied. The agent 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.  
   a. Select a check box that corresponds to the rule for which you want to change the order.  
   b. Click Reorder.  
   A box appears around the order number for the rule.  
   c. In the Priority column box, delete the existing order number and type a new one.  
   d. Click Save Reorder.  
      The rule moves to the priority level that you entered, and all the other rule order numbers change accordingly.  
      For example, if you select rule number 5 and change it to rule number 3, then rules number 1 and 2 remain the same, and rules numbered 3 and higher increase by one number. |
| Enable/Disable rules | Click the icon under the Enabled column. |
Types of Content Filtering Rules

You can create rules that filter email messages according to the conditions you specify or according to the email addresses of the sender or recipient. Conditions you can specify in the rule include: which header fields to scan, whether or not to search the body of an email message, and what keywords to search for.

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. For details, see Adding a Content Filtering Rule for Any Matching Condition on page 6-22.

• **Filter messages that match all conditions defined**: This type of rule is capable of filtering content from any message during a scan. For details, see Adding a Content Filtering Rule for All Matching Conditions on page 6-19.

  **Note**
  This rule type is not available for Manual and Scheduled Content Filtering Scans.

• **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 general content filter rules, except that they only filter content from specified email accounts. For details, see *Adding a Content Filtering Monitoring Rule on page 6-24.*

- **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. For details, see *Creating Exceptions to Content Filtering Rules on page 6-27.*

After you have created your rule, the Messaging Security Agent begins to filter all incoming and outgoing messages according to your rule. When a content violation occurs, the Messaging Security Agent takes action against the violating email message. The action that the Security Server takes also depends on the actions that you set in your rule.

### Adding a Content Filtering Rule for All Matching Conditions

This rule type is not available for Manual and Scheduled Content Filtering Scans.

**Procedure**

1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.
3. Click **Configure**.
   
   A new screen appears.
4. Click **Content Filtering**.
   
   A new screen appears.
5. Click **Add**.
   
   A new screen appears.
6. Select **Filter message that match all conditions defined**.
7. Click **Next**.
8. Type the name of your rule in the **Rule name** field.

9. Select the message part that you want to filter for undesirable content. The Messaging Security Agent can filter email messages by:
   - Header (From, To, and Cc)
   - Subject
   - Size of message body or attachment
   - Attachment file name

   **Note**
   The Messaging Security Agent only supports filtering of header and subject content during real-time scan.

10. Click **Next**.

11. Select an action for the Messaging Security Agent to take when it detects undesirable content. The Messaging Security Agent can perform the following actions (For descriptions, see *Scan Targets and Actions for Messaging Security Agents on page 7-15*):
   - Replace with text/file
   - Quarantine entire message
   - Quarantine message part
   - Delete entire message
   - Archive
   - Pass entire message

   **Note**
   You cannot replace text from the From, To, Cc, or subject fields.

12. Select **Notify recipients** to set the Messaging Security Agent to notify the intended recipients of email messages that had content filtered.
Select **Do not notify external recipients** to only send notifications to internal mail recipients. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

13. Select **Notify senders** to set the Messaging Security Agent to notify the senders of email messages that had content filtered.

Select **Do not notify external senders** to only send notifications to internal mail senders. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

14. In the **Advanced Options** section, click the plus (+) icon to expand the **Archive Setting** subsection.

   a. In the **Quarantine directory** field, type the path to the folder for Content Filtering to place quarantined email or accept the default value: `<Messaging Security Agent Installation folder>\storage\quarantine`

   b. In the **Archive directory** field, type the path to the folder for Content Filtering to place archived email or accept the default value: `<Messaging Security Agent Installation folder>\storage\backup for content filter`

15. Click the plus (+) icon to expand the **Replacement Settings** subsection.

   a. In the **Replacement file name** field, type the name of the file that Content Filtering will replace an email message with when a rule using the “Replace with text/file” action is triggered, or accept the default value.

   b. In the **Replacement text** field, type or paste the content of the replacement text for Content Filtering to use when an email message triggers a rule whose action is “Replace with text/file” or accept the default text.

16. Click **Finish**.

The wizard closes and returns to the Content Filtering screen.
Adding a Content Filtering Rule for Any Matching Condition

- For Real-time Scan:
  Security Settings > {Messaging Security Agent} > Configure > Content Filtering

- For Manual Scan:
  Scans > Manual > {Expand Messaging Security Agent} > Content Filtering

- For Scheduled Scan:
  Scans > Scheduled > {Expand Messaging Security Agent} > Content Filtering

Procedure

1. Click Add.
   A new screen appears.

2. Select Filter message that match any condition defined.

3. Click Next.

4. Type the name of your rule in the Rule name field.

5. Select the message part that you want to filter for undesirable content. The Messaging Security Agent can filter email messages by:
   - Header (From, To, and Cc)
   - Subject
   - Body
   - Attachment
6. Click Next.

7. Add keywords for the target part that you want to filter for undesirable content. For details on working with keywords, see Keywords on page D-5.
   a. If necessary, select whether or not to make content filter case-sensitive.
   b. Import new keyword files from a .txt file as needed.
   c. Define a list of synonyms.

8. Click Next.

9. Select an action for the Messaging Security Agent to take when it detects undesirable content. The Messaging Security Agent can perform the following actions (For descriptions, see Scan Targets and Actions for Messaging Security Agents on page 7-15):
   • Replace with text/file
     
     ____________
     
     Note
     You cannot replace text from the From, To, Cc, or subject fields.
     
     • Quarantine entire message
     • Quarantine message part
     • Delete entire message
     • Archive

10. Select Notify recipients to set the Messaging Security Agent to notify the intended recipients of email messages that had content filtered.

    Select Do not notify external recipients to only send notifications to internal mail recipients. Define internal addresses from Operations > Notification Settings > Internal Mail Definition.
11. Select **Notify senders** to set the Messaging Security Agent to notify the senders of email messages that had content filtered.

Select **Do not notify external senders** to only send notifications to internal mail senders. Define internal addresses from Operations > Notification Settings > Internal Mail Definition.

12. In the **Advanced Options** section, click the plus (+) icon to expand the **Archive Setting** subsection.

   a. In the **Quarantine directory** field, type the path to the folder for Content Filtering to place quarantined email or accept the default value: <Messaging Security Agent Installation folder>\storage\quarantine

   b. In the **Archive directory** field, type the path to the folder for Content Filtering to place archived email or accept the default value: <Messaging Security Agent Installation folder>\storage\backup for content filter

13. Click the plus (+) icon to expand the **Replacement Settings** subsection.

   a. In the **Replacement file name** field, type the name of the file that Content Filtering will replace an email message with when a rule using the “Replace with text/file” action is triggered, or accept the default value.

   b. In the **Replacement text** field, type or paste the content of the replacement text for Content Filtering to use when an email message triggers a rule whose action is “Replace with text/file” or accept the default text.

14. Click **Finish**.

   The wizard closes and returns to the Content Filtering screen.

---

**Adding a Content Filtering Monitoring Rule**

- For Real-time Scan:

  Security Settings > {Messaging Security Agent} > Configure > Content Filtering

- For Manual Scan:
Scans > Manual > {Expand Messaging Security Agent} > Content Filtering

• For Scheduled Scan:

Scans > Scheduled > {Expand Messaging Security Agent} > Content Filtering

Procedure

1. Click Add.
   A new screen appears.

2. Select **Monitor the message content of particular email accounts.**

3. Click Next.

4. Type the name of your rule in the **Rule name** field.

5. Set the email accounts to monitor.

6. Click Next.

7. Select the message part that you want to filter for undesirable content. The Messaging Security Agent can filter email messages by:
   • Subject
   • Body
   • Attachment

---

**Note**

The Messaging Security Agent only supports filtering of these parts of the email message during real-time scan. It does not support filtering of header and subject content during manual and scheduled scans.

---

8. Add keywords for the target part that you want to filter for undesirable content. For details on working with keywords, see *Keywords on page D-5.*
   a. If necessary, select whether or not to make content filter case-sensitive.
   b. Import new keyword files from a `.txt` file as needed.
c. Define a list of synonyms.

9. Click Next.

10. Select an action for the Messaging Security Agent to take when it detects undesirable content. The Messaging Security Agent can perform the following actions (For descriptions, see Scan Targets and Actions for Messaging Security Agents on page 7-15):

   • Replace with text/file

   ![Note]
   
   You cannot replace text from the From, To, Cc, or subject fields.

   • Quarantine entire message

   • Quarantine message part

   • Delete entire message

   • Archive

11. Select Notify recipients to set the Messaging Security Agent to notify the intended recipients of email messages that had content filtered.

    Select Do not notify external recipients to only send notifications to internal mail recipients. Define internal addresses from Operations > Notification Settings > Internal Mail Definition.

12. Select Notify senders to set the Messaging Security Agent to notify the senders of email messages that had content filtered.

    Select Do not notify external senders to only send notifications to internal mail senders. Define internal addresses from Operations > Notification Settings > Internal Mail Definition.

13. In the Advanced Options section, click the plus (+) icon to expand the Archive Setting subsection.

    a. In the Quarantine directory field, type the path to the folder for Content Filtering to place quarantined email or accept the default value: <Messaging Security Agent Installation folder>\storage\quarantine
b. In the **Archive directory** field, type the path to the folder for Content Filtering to place archived email or accept the default value: `<Messaging Security Agent Installation folder>\storage\backup for content filter`

14. Click the plus (+) icon to expand the **Replacement Settings** subsection.
   
a. In the **Replacement file name** field, type the name of the file that Content Filtering will replace an email message with when a rule using the “Replace with text/file” action is triggered, or accept the default value.

b. In the **Replacement text** field, type or paste the content of the replacement text for Content Filtering to use when an email message triggers a rule whose action is “Replace with text/file” or accept the default text.

15. Click **Finish**.

The wizard closes and returns to the Content Filtering screen.

---

### Creating Exceptions to Content Filtering Rules

- **For Real-time Scan:**

  Security Settings > {Messaging Security Agent} > Configure > Content Filtering

- **For Manual Scan:**

  Scans > Manual > {Expand Messaging Security Agent} > Content Filtering

- **For Scheduled Scan:**

  Scans > Scheduled > {Expand Messaging Security Agent} > Content Filtering

---

**Procedure**

1. Click **Add**.

   A new screen appears.
2. Select **Create exception for particular email accounts**.

3. Click **Next**.

4. Type a rule name.

5. Type the email accounts that you want to exempt from content filtering in the space provided and click **Add**.

   The email account is added to your list of exempt email accounts. The Messaging Security Agent does not apply content rules with a lower priority than this rule to email accounts in this list.

6. When you are satisfied with your list of email accounts, click **Finish**.

   The wizard closes and returns you to the **Content Filtering** screen.

---

**Data Loss Prevention**

Use Data Loss Prevention to protect against losing data through outgoing email. This feature can protect such data as social security numbers, telephone numbers, bank account numbers, and other confidential business information that matches a set pattern.

The following Microsoft Exchange versions are supported in this version:

**Table 6-3. Supported Microsoft Exchange Versions**

<table>
<thead>
<tr>
<th>SUPPORTED</th>
<th>NOT SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007 x64</td>
<td>2003 x86/x64</td>
</tr>
<tr>
<td>2010 x64</td>
<td>2007 x86</td>
</tr>
<tr>
<td></td>
<td>2010 x86</td>
</tr>
</tbody>
</table>

**Preparatory Work**

Before monitoring sensitive data for potential loss, determine the following:
• Which data needs protection from unauthorized users
• Where the data resides
• Where and how the data is transmitted
• Which users are authorized to access or transmit this information

This important audit typically requires input from multiple departments and personnel familiar with the sensitive information in your organization. The procedures below assume that you have identified the sensitive information and have established security policies regarding handling of confidential business information.

The Data Loss Prevention feature comprises three basic parts:
• **Rules** (patterns to search for)
• **Domains to exclude** from filtering
• **Approved Senders** (email accounts to exclude from filtering)

For details, see *Managing Data Loss Prevention Rules on page 6-29*.

**Managing Data Loss Prevention Rules**

The Messaging Security Agent displays all the Data Loss Prevention rules on the **Data Loss Prevention** screen (Security Settings > {Messaging Security Agent} > Configure > Data Loss Prevention).

**Procedure**

1. View summary information about the rules, including:
   • **Rule**: WFBS comes with default rules (see *Default Data Loss Prevention Rules on page 6-37*). These rules are disabled by default. You can modify these rules according to your requirements or delete them. If none of these rules meet your requirements, add your own rules.
Tip
Move your mouse pointer over the rule name to view the rule. Rules that use a regular expression are flagged with a magnifying glass ([^*2]+) icon.

- **Action**: The Messaging Security Agent takes this action when a rule is triggered.
- **Priority**: The Messaging Security Agent applies each rule in succession according to the order shown on this page.
- **Enabled**: A green icon indicates an enabled rule while a red icon indicates a disabled rule.

2. Perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable/Disable Data Loss Prevention</td>
<td>Select or clear <strong>Enable real-time Data Loss Prevention</strong> on top of the screen.</td>
</tr>
<tr>
<td>Add a rule</td>
<td>Click <strong>Add</strong>. A new screen opens where you can choose the type of rule to add. For details, see Adding Data Loss Prevention Rules on page 6-38.</td>
</tr>
<tr>
<td>Modify a rule</td>
<td>Click the rule name. A new screen opens. For details about rule settings that you can modify, see Adding Data Loss Prevention Rules on page 6-38.</td>
</tr>
<tr>
<td><strong>TASK</strong></td>
<td><strong>STEPS</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Import and export rules | Import one or more rules from (or export them to) a plain-text file, as shown below. If you prefer, you can then edit rules directly by using this file.  

[SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599]  
RuleName=Bubbly  
UserExample=  
Value=Bubbly  

[SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6]  
RuleName=Master Card No.  
UserExample=Value=.REG. \b5\{1-5\}\d\{2\}\-?\x20?\d\{4\}\-?\x20?\d\{4\}\-?\x20?\d\{4\}\b |  

To export rules to a plain-text file, select one or more rules in the list and then click **Export**.  

**Tip**  
You can select rules that appear on one screen only. To select rules that currently appear on different screens, increase the "Rows per page" value at the top of the Rule list table to display enough rows to encompass all of the rules to export.
<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>To import rules:</td>
<td></td>
</tr>
<tr>
<td>a.</td>
<td>Create a plain-text file in the format shown above. You can also click Download more default rules below the table and then save the rules.</td>
</tr>
<tr>
<td>b.</td>
<td>Click <strong>Import</strong>.</td>
</tr>
<tr>
<td></td>
<td>A new window opens.</td>
</tr>
<tr>
<td>c.</td>
<td>Click <strong>Browse</strong> to locate the file to import, and then click <strong>Import</strong>.</td>
</tr>
<tr>
<td></td>
<td>Data Loss Prevention imports the rules in the file and appends them to the end of the current rules list.</td>
</tr>
</tbody>
</table>

---

**Tip**

If you already have more than 10 rules, the imported rules will not be visible on the first page. Use the page-navigation icons at the top or bottom of the rules list to display the last page of the list. The newly imported rules should be there.
### Reorder rules

The Messaging Security Agent applies the Data Loss Prevention rules to email messages according to the order shown in the **Data Loss Prevention** screen. Configure the order in which the rules are applied. The agent 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 Data Loss Prevention.

1. 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. In the **Priority** column box, delete the existing order number and type a new one.

   **Note**

   Be sure to enter a number no larger than the total number of rules in the list. If you enter a number higher than the total number of rules, WFBS disregards the entry and does not change the order of the rule.

4. Click **Save Reorder**.
   - The rule moves to the priority level that you entered, and all the other rule order numbers change accordingly.

   For example, if you select rule number 5 and change it to rule number 3, then rules number 1 and 2 remain the same, and rules numbered 3 and higher increase by one number.

### Enable/Disable rules

Click the icon under the **Enabled** column.
### Task: Remove rules

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you delete a rule, the Messaging Security Agent updates the order of the other rules to reflect the change.</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>Deleting a rule is irreversible, consider disabling a rule instead of deleting.</td>
</tr>
<tr>
<td>a. Select a rule.</td>
<td></td>
</tr>
<tr>
<td>b. Click <strong>Remove</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

For more information, refer to the [Worry-Free Business Security 8.0 Administrator’s Guide](#).
**Exclude specific domain accounts**

Within the walls of a company, the exchange of confidential business information is a necessary daily occurrence. Also, the processing load on Security Servers would be extreme if Data Loss Prevention had to filter all internal messages. For these reasons, you need to set up one or more default domains, representing your internal company mail traffic, so that Data Loss Prevention does not filter messages sent from one email account to another within your company domain.

This list allows all internal email messages (within your company domain) to bypass Data Loss Prevention rules. At least one such domain is required. Add to the list if you use more than one domain.

For example: *@example.com*

a. Click the plus (+) icon to expand the **Specific Domain Account(s) excluded from Data Loss Prevention** section.

b. Place your cursor in the **Add** field and type the domain, using the following pattern: *@example.com*

c. Click **Add**.

   The domain appears in the list shown below the **Add** field.

d. Click **Save** to complete the process.

---

**WARNING!**

Data Loss Prevention does not add your domain until you click **Save**. If you click **Add** but not **Save**, your domain will not be added.
<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add email accounts to the Approved Senders List</td>
<td>Mail from approved senders travels outside of your network with no filtering by Data Loss Prevention. Data Loss Prevention will ignore the content of any mail sent from email accounts on the approved list.</td>
</tr>
<tr>
<td></td>
<td>a. Click the plus (+) icon to expand the Approved Senders section.</td>
</tr>
<tr>
<td></td>
<td>b. Place your cursor in the Add field and type the full email address, using the following pattern: <code>example@example.com</code></td>
</tr>
<tr>
<td></td>
<td>c. Click Add. The address appears in the list shown below the Add field.</td>
</tr>
<tr>
<td></td>
<td>d. Click Save to complete the process.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Data Loss Prevention does not add the address until you click Save. If you click Add but not Save, the address will not be added.</td>
</tr>
<tr>
<td>Import email accounts to the Approved Senders List</td>
<td>You can import a list of email addresses from a plain-text file formatted with one email account per line, such as: <code>admin@example.com</code> <code>ceo@example.com</code> <code>president@example.com</code></td>
</tr>
<tr>
<td></td>
<td>a. Click the plus (+) icon to expand the Approved Senders section.</td>
</tr>
<tr>
<td></td>
<td>b. Click Import. A new window opens.</td>
</tr>
<tr>
<td></td>
<td>c. Click Browse to locate the plain-text file to import, and then click Import. Data Loss Prevention imports the rules in the file and appends them to the end of the current list.</td>
</tr>
</tbody>
</table>
3. Click **Save**.

---

**Default Data Loss Prevention Rules**

Data Loss Prevention comes with a few default rules, as shown in the following table.

**Table 6-4. Default Data Loss Prevention Rules**

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Example</th>
<th>Regular Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa Card account number</td>
<td>4111-1111-1111-1111</td>
<td>.REG. \b4\d{3}-?\x20?\d{4}-?\x20?\d{4}-?\x20?\d{4}b</td>
</tr>
<tr>
<td>MasterCard account number</td>
<td>5111-1111-1111-1111</td>
<td>.REG. \b5[1-5]\d{2}-?\x20?\d{4}-?\x20?\d{4}-?\x20?\d{4}b</td>
</tr>
<tr>
<td>American Express account number</td>
<td>3111-111111-1111</td>
<td>.REG. \b3[4,7]\d{2}-?\x20?\d{6}-?\x20?\d{5}b</td>
</tr>
<tr>
<td>Diners Club/ Carte Blanche account number</td>
<td>3111-111111-1111</td>
<td>.REG. [^d-][(36\d{2})</td>
</tr>
<tr>
<td>IBAN</td>
<td>BE68 5390 0754 7034, FR14</td>
<td>.REG. [^w-]([A-Z][(2)\d{2}][-</td>
</tr>
<tr>
<td>ISO date</td>
<td>2004/01/23, 04/01/23, 2004-01-23, 04-01-23</td>
<td>.REG. [^dV-][1-2]\d{3}[-V][0-1]?\d[-V][0-3]?\d\d{2}[-V][0-1]?\d[-V] [0-3]?\d[^dV-]</td>
</tr>
</tbody>
</table>

**Note**

A zip file containing more DLP rules can be downloaded from the web console. Navigate to **Security Settings** > {Messaging Security Agent} > **Configure** > **Data Loss Prevention** and click **Download more default rules**.
Adding Data Loss Prevention Rules

Procedure

1. Navigate to **Security Settings**.

2. Select a Messaging Security Agent.

3. Click **Configure**.
   
   A new screen appears.

4. Click **Data Loss Prevention**.
   
   A new screen appears.

5. Click **Add**.
   
   A new screen appears.

6. Select the message part that you want to evaluate. The Messaging Security Agent can filter email messages by:
   
   • Header (From, To, and Cc)
   
   • Subject
   
   • Body
   
   • Attachment

7. Add a rule.

   **To add a rule based on a keyword:**

   a. Select **Keyword**.

   b. Type the keyword in the field shown. The keyword must be from 1 to 64 alphanumeric characters long.

   c. Click **Next**.

   **To add a rule based on auto-generated expressions:**
a. See *Regular Expressions on page D-9* for guidelines on defining regular expressions.

b. Select **Regular expression (auto-generated)**.

c. In the provided field type a **Rule Name**. This field is required.

d. In the **Example** field, type or paste an example of the kind of string (up to 40 characters long) that the regular expression is intended to match. The alphanumeric characters appear in all caps in the shaded area with rows of boxes beneath the **Example** field.

e. If there are any constants in the expression, select them by clicking the boxes in which the characters are displayed.

As you click each box, its border turns red to indicate that it is a constant and the auto-generation tool modifies the regular expression shown below the shaded area.

---

**Note**

Non-alphanumeric characters (such as spaces, semicolons, and other punctuation marks) are automatically considered constants and cannot be toggled into variables.

---

f. To verify that the generated regular expression matches the intended pattern, select **Provide another example to verify the rule (Optional)**.

A test field appears below this option.

g. Type another example of the pattern that you just entered.

For example, if this expression is to match a series of account numbers of the pattern “01-EX????? 20??”, then type another example that matches, such as “01-Extreme 2010” and then click **Test**.

The tool validates the new sample against the existing regular expression and places a green check mark icon next to the field if the new sample matches. If the regular expression does not match the new sample, a red X icon appears next to the field.
WARNING!

Regular expressions created using this tool are case-insensitive. These expressions can match only patterns with the exact same number of characters as your sample; they cannot evaluate a pattern of “one or more” of a given character.

h. Click Next.

To add a rule based on user-defined expressions:

WARNING!

Regular expressions are a powerful string-matching tool. Ensure that you are comfortable with regular expression syntax before using these expressions. Poorly written regular expressions can dramatically impact performance. Trend Micro recommends starting with simple regular expressions. When creating new rules, use the “archive” action and observe how Data Loss Prevention manages messages using the rule. When you are confident that the rule has no unexpected consequences, you can change the action.

a. See Regular Expressions on page D-9 for guidelines on defining regular expressions.

b. Select Regular expression (user-defined).

A Rule Name and Regular Expression field display.

c. In the provided field type a Rule Name. This field is required.

d. In the Regular Expression field type a regular expression, beginning with a “.REG.” prefix, up to 255 characters long including the prefix.

WARNING!

Be very careful when pasting into this field. If any extraneous characters, such as an OS-specific line feed or an HTML tag, is included in the content of your clipboard, the expression pasted will be inaccurate. For this reason, Trend Micro recommends typing the expression by hand.

e. To verify that the regular expression matches the intended pattern, select Provide another example to verify the rule (Optional).
A test field appears below this option.

f. Type another example of the pattern that you just entered (40 characters or less).

For example, if this expression is to match a series of account numbers of the pattern “ACC-????? 20??” type another example that matches, such as “Acc-65432 2012” and then click Test.

The tool validates the new sample against the existing regular expression and places a green check mark icon next to the field if the new sample matches. If the regular expression does not match the new sample, a red X icon appears next to the field.

g. Click Next.

8. Select an action for the Messaging Security Agent to take when a rule is triggered (For descriptions, see Scan Targets and Actions for Messaging Security Agents on page 7-15):
   • Replace with text/file
   • Quarantine entire message
   • Quarantine message part
   • Delete entire message
   • Archive
   • Pass entire message

9. Select Notify recipients to set the Messaging Security Agent to notify the intended recipients when Data Loss Prevention takes action against a specific email message.

For various reasons, you may want to avoid notifying external mail recipients that a message containing sensitive information was blocked. Select Do not notify external recipients to only send notifications to internal mail recipients. Define
internal addresses from **Operations** > **Notification Settings** > **Internal Mail Definition**.

**10.** Select **Notify senders** to set the Messaging Security Agent to notify the intended senders when Data Loss Prevention takes action against a specific email message.

For various reasons, you may want to avoid notifying external mail senders that a message containing sensitive information was blocked. Select **Do not notify external senders** to only send notifications to internal mail senders. Define internal addresses from **Operations** > **Notification Settings** > **Internal Mail Definition**.

**11.** In the **Advanced Options** section, click the plus (+) icon to expand the **Archive Setting** subsection.

a. In the ** Quarantine directory** field, type the path to the folder for Data Loss Prevention to place quarantined email or accept the default value: `<Messaging Security Agent Installation folder>\storage \quarantine`

b. In the **Archive directory** field, type the path to the folder for Data Loss Prevention to place archived email or accept the default value: `<Messaging Security Agent Installation folder>\storage\backup for content filter`

**12.** Click the plus (+) icon to expand the **Replacement Settings** subsection.

a. In the **Replacement file name** field, type the name of the file that Data Loss Prevention will replace an email message with when a rule using the “Replace with text/file” action is triggered, or accept the default value.

b. In the **Replacement text** field, type or paste the content of the replacement text for Data Loss Prevention to use when an email message triggers a rule whose action is “Replace with text/file” or accept the default text.

**13.** Click **Finish**.

The wizard closes and returns to the Data Loss Prevention screen.
Attachment Blocking

Attachment blocking prevents attachments in email messages from 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.

Configuring Attachment Blocking

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

- For Real-time Scan:
  
  Security Settings > {Messaging Security Agent} > Configure > Attachment Blocking

- For Manual Scan:
  
  Scans > Manual > {Expand Messaging Security Agent} > Attachment Blocking
• For Scheduled Scan:

Scans > Scheduled > {Expand Messaging Security Agent} > Attachment Blocking

---

**Procedure**

1. From the **Target** tab, update the following as required:

   • **All attachments**: The 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.

   • **Attachment types to exclude**

   • **Attachment names to exclude**

   • **Specific attachments**: When you select this type of scan, the 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.

   • **Attachment types**: The agent examines the file header rather than the file name to ascertain the actual file type.

   • **Attachment names**: By default, the 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 agent will detect attachment types according to their name.

   • **Block attachment types or names within ZIP files**

2. Click the **Action** tab to set the actions that the Messaging Security Agent takes when it detects attachments. The Messaging Security Agent can perform the following actions (For descriptions, see *Scan Targets and Actions for Messaging Security Agents on page 7-15*):

   • Replace with text/file

   • Quarantine entire message
• Quarantine message part
• Delete entire message

3. Select **Notify recipients** to set the Messaging Security Agent to notify the intended recipients of email messages that have attachments.

Select **Do not notify external recipients** to only send notifications to internal mail recipients. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

4. Select **Notify senders** to set the Messaging Security Agent to notify the senders of email messages that have attachments.

Select **Do not notify external senders** to only send notifications to internal mail senders. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

5. Click the plus (+) icon to expand the **Replacement Settings** subsection.
   a. In the **Replacement file name** field, type the name of the file that Attachment Blocking will replace an email message with when a rule using the “Replace with text/file” action is triggered, or accept the default value.
   b. In the **Replacement text** field, type or paste the content of the replacement text for Attachment Blocking to use when an email message triggers a rule whose action is “Replace with text/file” or accept the default text.

6. Click **Save**.

---

**Web Reputation**

Web Reputation helps prevent access to URLs on the web or embedded in email messages that pose security risks. Web Reputation checks the URL’s reputation against the Trend Micro web reputation servers and then correlates the reputation with the specific web reputation policy enforced on the client. Depending on the policy in use:

• The Security Agent will block or allow access to the website.
The Messaging Security Agent (Advanced only) will quarantine, delete, or tag the email message containing malicious URLs, or allow the message to be sent if the URLs are safe.

Web Reputation provides both email notification to the administrator and online notification to the user for detections.

For Security Agents, configure a different level of security based on the location (In Office/Out of Office) of the client.

If Web Reputation blocks a URL and you feel the URL is safe, add the URL to the Approved URLs list.

Tip
To save network bandwidth, Trend Micro recommends adding the enterprise internal websites to the Web reputation approved URL list.

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 if its score falls within a defined threshold, and safe if its score exceeds the threshold.

A Security Agent has three security levels that determine whether it will allow or block access to a URL.

- **High**: Blocks pages that are:
  - **Dangerous**: Verified to be fraudulent or known sources of threats
  - **Highly suspicious**: Suspected to be fraudulent or possible sources of threats
  - **Suspicious**: Associated with spam or possibly compromised
  - **Untested**: While Trend Micro actively tests web pages for safety, users may encounter untested pages when visiting new or less popular websites. Blocking access to untested pages can improve safety but can also prevent access to safe pages.

- **Medium**: Blocks pages that are:
Managing Basic Security Settings for Messaging Security Agents (Advanced Only)

- **Dangerous**: Verified to be fraudulent or known sources of threats
- **Highly suspicious**: Suspected to be fraudulent or possible sources of threats
- **Low**: Blocks pages that are:
  - **Dangerous**: Verified to be fraudulent or known sources of threats

Configuring Web Reputation for Messaging Security Agents

**Procedure**

1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.
3. Click **Configure**.
   
   A new screen appears.
4. Click **Web Reputation**.
   
   A new screen appears.
5. Update the following as required:
   - **Enable Web Reputation**
   - **Security Level**: **High**, **Medium**, or **Low**
   - **Approved URL(s)**
     - **URLs to approve**: Separate multiple URLs with semicolons (;). Click **Add**.

**Note**

- Approving a URL implies approving all its sub domains.
- Use wildcards with caution as they may allow large sets of URLs.

- **Approved URL list**: URLs in this list will not be blocked.
6. Click the **Action** tab and select an action for the Messaging Security Agent to take when a web reputation policy is triggered (For descriptions, see *Scan Targets and Actions for Messaging Security Agents on page 7-15*):

- Replace with text/file

    **Note**
    You cannot replace text from the From, To, Cc, or subject fields.

- Quarantine message to user’s spam folder
- Delete entire message
- Tag and deliver

7. Select **Take action on URLs that have not been assessed by Trend Micro** to treat unclassified URLs as suspicious. The same action specified in the previous step will be performed on email messages containing unclassified URLs.

8. Select **Notify recipients** to set the Messaging Security Agent to notify the intended recipients when Web Reputation takes action against a specific email message.

    For various reasons, you may want to avoid notifying external mail recipients that a message containing malicious URLs was blocked. Select **Do not notify external recipients** to only send notifications to internal mail recipients. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

9. Select **Notify senders** to set the Messaging Security Agent to notify the intended senders when Web Reputation takes action against a specific email message.

    For various reasons, you may want to avoid notifying external mail senders that a message containing malicious URLs was blocked. Select **Do not notify external senders** to only send notifications to internal mail senders. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

10. Click **Save**.
Quarantine for Messaging Security Agents

When the Messaging Security Agent detects a threat, spam, restricted attachment and/or restricted content in email messages, the agent can move the message to a quarantine folder. This process acts as an alternative to message/attachment deletion and prevents users from opening the infected message and spreading the threat.

The default quarantine folder on the Message Security Agent is:

<Messaging Security Agent installation folder>\storage \quarantine

Quarantined files are encrypted for added security. To open an encrypted file, use the Restore Encrypted Virus (VSEncode.exe) tool. See Restoring Encrypted Files on page 14-9.

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 a 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.
Querying Quarantine Directories

Procedure

1. Navigate to Security Settings.

2. Select a Messaging Security Agent.

3. Click Configure.

   A new screen appears.

4. Click Quarantine > Query.

   A new screen appears.

5. Update the following as required:
   - Date/Time Range
   - 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.

6. Click **Search**. See *Viewing Query Results and Taking Action on page 6-51*.

### Viewing Query Results and Taking Action

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. Administrators can decrypt the file using VSEncoder.exe (See *Restoring Encrypted Files on page 14-9*) and then rename it to `.eml` to view it.

![WARNING!]

Viewing infected files could spread the infection.

- **Resend status**

### Procedure

1. If you feel that a message is unsafe, delete the message.

![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.
2. If you feel that a message is safe, select the message and click the resend icon (衷).

---

**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.

---

3. If you are unable to resend the message, it is possible that the system administrator’s account on the Microsoft Exchange server does not exist.

   a. Using the Windows Registry Editor, open the following registry entry on the server:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion
   ```

   b. 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}`
     
     Example: `admin@example.com`

   - ResendMailboxDomain `{Administrator’s Domain}`
     
     Example: `example.com`

   - ResendMailSender `{Administrator’s Email Account}`
     
     Example: `admin`

   c. Close the Registry Editor.
Maintaining Quarantine Directories

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

Procedure

1. Navigate to Security Settings.
2. Select a Messaging Security Agent.
3. Click Configure.
   
   A new screen appears.
4. Click Quarantine > Maintenance.
   
   A new screen appears.
5. 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.
6. Click Save.
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.

The Messaging Security Agent quarantines email messages according to configured actions. The following are the quarantine directories:

- **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.

By default, all directories have the same paths (\<Messaging Security Agent installation folder\>\storage\quarantine). You can change the paths for each or all of the directories.

**Procedure**

1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.
3. Click **Configure**.
   
   A new screen appears.
4. Click **Quarantine > Directory**.
   
   A new screen appears.
5. Set the path for the following quarantine directories:
• Antivirus
• Anti-Spam
• Content Filtering
• Attachment Blocking

6. Click Save.

Notification Settings for Messaging Security Agents

WFBS can send notifications in the form of email messages to various alerts.

You can configure notifications to apply only to internal email messages by using Custom Internal Email Definitions. This is 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.

About Custom Internal Email Definitions

The Messaging Security Agent divides email traffic into two network categories: internal and external. The agent queries the Microsoft Exchange server to learn how the internal and external addresses are defined. All internal addresses share a common domain and all external addresses do not belong to that domain.

For example, if the internal domain address is “@trend_1.com”, then the Messaging Security Agent classifies addresses such as “abc@trend_1.com” and “xyz@trend_1.com” as internal addresses. The agent classifies all other addresses, such as “abc@trend_2.com” and “jondoe@123.com” as external.
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.

### Configuring Notification Settings for Messaging Security Agents

#### Procedure

1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.
3. Click **Configure**.
   
   A new screen appears.
4. Click **Operations > Notification Settings**.
   
   A new screen appears.
5. Update the following as required:
   
   - **Email address**: The address on behalf of whom WFBS will send notification messages.
   
   - **Internal Email Definition**
     
     - **Default**: WFBS will treat email messages from the same domain as Internal Emails.
• **Custom**: Specify individual email addresses or domains to treat as internal email messages.

6. Click **Save**.

---

### Configuring Spam Maintenance

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

**Procedure**

1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.
3. Click **Configure**.
   
   A new screen appears.
4. Click **Operations > Spam Maintenance**.
   
   A new screen appears.
5. Click **Enable End User Quarantine tool**.

When you enable the tool, a quarantine folder is created on the server-side of each client's mailbox and a **Spam Mail** folder appears in the end user's Outlook folder tree. After EUQ is enabled and the Spam Mail folders are created, EUQ will filter spam mail to the user's Spam mail folder. For details, see *Managing the End User Quarantine on page 6-58*.

---

**Tip**

If you select this option, Trend Micro recommends disabling the Trend Micro Anti-Spam toolbar option on agents to increase performance on clients.

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

6. Click **Create spam folder and delete spam messages** to create (immediately) Spam Mail folders for newly created mail clients and for existing mail clients that have deleted their Spam Mail folder. For other existing mail clients, it will delete spam messages that are older than the days specified in the Client Spam Folder Settings field.

7. In **Delete spam messages older than {number} days**, modify the length of time that the Messaging Security Agent will retain spam messages. The default value is 14 days and the maximum time limit is 30 days.

8. To disable the End User Quarantine tool for select users:
   a. Under **End User Quarantine tool exception list**, type the email address of the end user for whom you want to disable EUQ.
   b. Click **Add**.

      The end user’s email address is added to the list of addresses that have EUQ disabled.

      To remove an end user from the list and restore the EUQ service, select the end user’s email address from the list and click **Delete**.

9. Click **Save**.

---

**Managing the End User Quarantine**

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 *Configuring Spam Maintenance on page 6-57*.

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.

**Client-side Spam Mail Folder**

End users can open email messages quarantined in the spam folder. When they open one of these messages, two buttons appear on the actual email message: **Approved Sender** and **View Approved Sender List**.

• When an end user opens an email message from the Spam Mail folder and clicks **Approved Sender**, then the sender's address for that email is added to the end user's **Approved Senders** list.

• Clicking **View Approved Sender List** opens another screen which allows the end user to view and modify their list of approved senders by email address or domain.

**Approved Senders**

When the end user receives an email message in the Spam Mail folder and clicks **Approve Sender**, the Messaging Security Agent moves the message to the end user's local inbox and adds the sender's address to the end user's personal Approved Sender List. The Messaging Security Agent logs the event.

When the Microsoft Exchange server receives messages from the addresses on the end user's Approved Senders list, it delivers them to the end user's inbox, regardless of the header or content of the message.

---

**Note**

The Messaging Security Agent 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.

**Trend Micro Support/Debugger**

The Support/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 Agent inserts messages into the program, and then records the action into log files upon execution. You can forward the logs to Trend Micro Technical Support staff to help them debug the actual program flow in your environment.

Use the debugger to generate logs on the following modules:

- Messaging Security Agent Master Service
- Messaging Security Agent Remote Configuration Server
- Messaging Security Agent System Watcher
- Virus Scan API (VSAPI)
- Simple Mail Transfer Protocol (SMTP)
- Common Gateway Interface (CGI)

By default, the MSA keeps the logs in the following directory:

`<Messaging Security Agent installation folder>\Debug`

View the output with any text editor.
Generating System Debugger Reports

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

Procedure

1. Navigate to **Security Settings**.
2. Select a Messaging Security Agent.
3. Click **Configure**.
   
   A new screen appears.
4. Click **Operations > Support/Debugger**.
   
   A new screen appears.
5. 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)
6. Click **Apply**.

   The debugger starts collecting data for the selected modules.

Real-time Monitor

The Real-time Monitor displays current information about the selected Microsoft Exchange Server and its Messaging Security Agent. It shows information about scanned messages and protection statistics, including the number of viruses and spam found,
attachments blocked, and content violations. It also checks whether the agent is working properly.

**Working with Real-time Monitor**

**Procedure**

1. To access Real-time Monitor from the web console:
   a. Navigate to **Security Settings**.
   b. Select an agent.
   c. Click **Configure**.
      A new screen appears.
   d. Click the **Real-time Monitor** link on the upper right portion of the screen.

2. To access Real-time Monitor from the Windows Start Menu, click **All Programs > Trend Micro Messaging Security Agent > Real-time Monitor**.

3. Click **Reset** to reset the protection statistics to zero.

4. Click **Clear Content** to clear older information about scanned messages.

**Adding a Disclaimer to Outbound Email Messages**

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

**Procedure**

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 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

Managing Scans

This chapter describes how to run scans on Security Agents and Messaging Security Agents (Advanced only) to protect your network and clients from threats.
About Scans

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

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

Worry-Free Business Security provides three types of scans. Each scan has a different purpose and use, but all are configured approximately the same way.

- Real-time Scan. See Real-time Scan on page 7-2 for details.
- Manual Scan. See Manual Scan on page 7-3 for details.
- Scheduled Scan. See Scheduled Scan on page 7-6 for details.

Security Agents use one of two scan methods when running scans:

- Smart scan
- Conventional scan

See Scan Methods on page 5-3 for details.

Real-time Scan

Real-time Scan is a persistent and ongoing scan.

Each time a file is opened, downloaded, copied, or modified, Real-time Scan in the Security Agent scans the file for threats. For details on configuring Real-time Scan, see Configuring Real-time Scan for Security Agents on page 5-7.

In the case of email messages, Real-time Scan in the Messaging Security Agent (Advanced only) guards all known virus entry points by scanning all incoming messages,
SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers. For details on configuring Real-time Scan, see Configuring Real-time Scan for Messaging Security Agents on page 6-5.

Manual Scan

Manual Scan is an on-demand scan.

Manual Scan on Security Agents eliminates threats from files and eradicates old infections, if any, to minimize reinfection.

Manual Scan on Messaging Security Agents (Advanced only) scans all the files in the Information Store of your Microsoft Exchange server.

The time taken for the scan depends on the client’s hardware resources and the number of files to be scanned. A Manual Scan in progress can be stopped by the Security Server administrator if the scan was run remotely from the web console, or by the user if the scan was run directly on the client.

Tip

Trend Micro recommends running Manual Scans after a threat outbreak.

Running Manual Scans

This procedure describes how Security Server administrators can run Manual Scan on Security Agents and Messaging Security Agents (Advanced only) from the web console.

Note

Manual Scan can also be run directly from clients by right-clicking the Security Agent icon in the Windows Task Bar and clicking Scan Now. It is not possible to run Manual Scan directly on Microsoft Exchange servers.
Procedure

1. Navigate to **Scans > Manual Scan**.
2. (Optional) Customize scan settings before running Manual Scan.

<table>
<thead>
<tr>
<th><strong>INSTRUCTIONS AND NOTES</strong></th>
<th><strong>RECOMMENDED SCAN SETTINGS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>To customize scan settings for the <strong>Security Agent</strong>, click a desktop or server group. See <em>Scan Targets and Actions for Security Agents on page 7-8.</em></td>
<td><strong>Target</strong></td>
</tr>
<tr>
<td></td>
<td>• All scannable files: Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.</td>
</tr>
<tr>
<td></td>
<td>• Scan compressed files up to 1 compression layers: Scans compressed files that are 1 compression layers deep. Default is &quot;off&quot; for the default server group and &quot;on&quot; for the default desktop group.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td><strong>Exclusions</strong></td>
</tr>
<tr>
<td>Scan settings for Security Agents are also used when users run Manual Scan directly from clients. However, if you grant users the privilege to configure their own scan settings, the user-configured settings will be used during the scan.</td>
<td>• Do not scan the directories where Trend Micro products are installed</td>
</tr>
<tr>
<td></td>
<td><strong>Advanced Settings</strong></td>
</tr>
<tr>
<td></td>
<td>• Modify Spyware/Grayware Approved List (for Anti-spyware only)</td>
</tr>
</tbody>
</table>
To customize scan settings for the **Messaging Security Agent**, expand an agent and click the following:

- **Antivirus**: Click to have the agent scan for viruses and other malware. See *Scan Targets and Actions for Messaging Security Agents on page 7-15*.
- **Content Filtering**: Click to have the agent scan email for prohibited content. See *Managing Content Filtering Rules on page 6-15*.
- **Attachment Blocking**: Click to have the agent scan email for attachment rule violations. See *Configuring Attachment Blocking on page 6-43*.

The agent scans all scannable files. It includes the message bodies of email messages in the scan.

- When the agent detects a file with a virus or other malware, it cleans the file. When it cannot clean the file, it replaces with text/file instead.
- When the agent detects a file with a Trojan or worm, it replaces the Trojan or worm with a text or file.
- When the agent detects a file with a Packer, it replaces the Packer with a text or file.
- The agent does not clean infected compressed files. This reduces the time required during real-time scanning.

3. Select the groups or Messaging Security Agents to scan.

4. Click **Scan Now**.

The Security Server sends a notification to agents to run Manual Scan. The Scan Notifying Results screen that appears shows you the number of agents that received and did not receive the notification.

5. To stop scans that are in progress, click **Stop Scanning**.

The Security Server sends another notification to agents to stop Manual Scan. The Stop Scan Notifying Results screen that appears shows you the number of agents that received and did not receive the notification. Security Agents may fail to receive the notification if they have become offline since running the scan or if there are network interruptions.
Scheduled Scan

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

**Tip**
Run Scheduled Scans during off-peak hours to minimize any potential disruptions to users and the network.

Configuring Scheduled Scans

Trend Micro recommends that you do not schedule a scan at the same time as a scheduled update. This may cause the Scheduled Scan to stop prematurely. Similarly, if you begin a Manual Scan when a Scheduled Scan is running, the scan stops, but will run again according to its schedule.

**Procedure**

1. Navigate to **Scans > Scheduled Scan**.
2. Click the **Schedule** tab.
   a. Configure the scan frequency (daily, weekly, or monthly) and start time. Each group or Messaging Security Agent can have its own schedule.
   
   **Note**
   For monthly Scheduled Scans, if you select 31, 30, or 29 days and a month has less than the number of days, the scan will not run that month.

   b. (Optional) Select **Shut down the client after completing a Scheduled Scan**.

   c. Click **Save**.
3. (Optional) Click the **Settings** tab to customize Scheduled Scan settings.
To customize scan settings for the **Security Agent**, click a desktop or server group. See *Scan Targets and Actions for Security Agents on page 7-8.*

**Note**
If you grant users the privilege to configure their own scan settings, the user-configured settings will be used during the scan.

<table>
<thead>
<tr>
<th><strong>INSTRUCTIONS AND NOTES</strong></th>
<th><strong>RECOMMENDED SCAN SETTINGS</strong></th>
</tr>
</thead>
</table>
| To customize scan settings for the **Security Agent**, click a desktop or server group. See *Scan Targets and Actions for Security Agents on page 7-8.* | **Target**  
  - All scannable files: Includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.  
  - Scan compressed files up to 2 compression layers: Scans compressed files that are 1 compression layers deep. |
| **Note** If you grant users the privilege to configure their own scan settings, the user-configured settings will be used during the scan. | **Exclusions**  
  - Do not scan the directories where Trend Micro products are installed |
| **Advanced Settings**  
  - Scan boot area (for Antivirus only)  
  - Modify Spyware/Grayware Approved List (for Anti-spyware only) |
To customize scan settings for the **Messaging Security Agent**, expand an agent and click the following:

- **Antivirus**: Click to have the agent scan for viruses and other malware. See *Scan Targets and Actions for Messaging Security Agents on page 7-15*.
- **Content Filtering**: Click to have the agent scan email for prohibited content. See *Managing Content Filtering Rules on page 6-15*.
- **Attachment Blocking**: Click to have the agent scan email for attachment rule violations. See *Configuring Attachment Blocking on page 6-43*.

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

4. Select the groups or Messaging Security Agents that will apply the Scheduled Scan settings.

**Note**

To disable Scheduled Scan, clear the check box for the group or Messaging Security Agent.

5. Click **Save**.

### Scan Targets and Actions for Security Agents

Configure the following settings for each scan type (Manual Scan, Scheduled Scan, and Real-time Scan):
Target Tab

- Scan Targets
- Scan Exclusions
- Advanced Settings
- Spyware/Grayware Approved List

Action Tab

- Scan Actions/ActiveAction
- Advanced Settings

Scan Targets

Select scan targets:

- **All scannable files**: includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.

  **Note**
  
  This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.

- **IntelliScan**: Scans files based on true-file type. See *IntelliScan on page D-2*.

- **Scan files with the following extensions**: Manually specify the files to scan based on their extensions. Separate multiple entries with commas.

Scan Exclusions

The following settings are configurable:

- Enable or disable exclusions
- Exclude Trend Micro product directories from scans
- Exclude other directories from scans
All subdirectories in the directory path you specify will also be excluded.

- Exclude file names or file names with full path from scans

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

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

### Advanced Settings (Scan Targets)

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time Scan, Manual Scan</td>
<td>Scan mapped drives and shared folders on the network: Select to scan directories physically located on other computers, but mapped to the local computer.</td>
</tr>
<tr>
<td>Real-time Scan</td>
<td>Scan compressed files: Up to __ compression layers (up to 6 layers)</td>
</tr>
<tr>
<td>Real-time Scan</td>
<td>Scan floppy during system shutdown</td>
</tr>
<tr>
<td>Real-time Scan</td>
<td>Enable IntelliTrap: IntelliTrap detects malicious code, such as bots, in compressed files. See <em>IntelliTrap on page D-2</em>.</td>
</tr>
</tbody>
</table>
### Managing Scans

<table>
<thead>
<tr>
<th>Scan Type</th>
<th>Option</th>
</tr>
</thead>
</table>
| Real-time Scan | Condition/Scan Trigger:  
  • **Read**: Scans files whose contents are read; files are read when they are opened, executed, copied, or moved.  
  • **Write**: Scans files whose contents are being written; a file’s contents are written when the file is modified, saved, downloaded, or copied from another location.  
  • **Read or write** |
| Manual Scan, Scheduled Scan | CPU Usage/Scan Speed: The Security Agent can pause after scanning one file and before scanning the next file.  
  Select from the following options:  
  • **High**: No pausing between scans  
  • **Medium**: Pause between file scans if CPU consumption is higher than 50%, and do not pause if 50% or lower  
  • **Low**: Pause between file scans if CPU consumption is higher than 20%, and do not pause if 20% or lower |
| Real-time Scan, Manual Scan, Scheduled Scan | Modify Spyware/Grayware Approved List. |
| Manual Scan, Scheduled Scan | Run advanced cleanup: The Security Agent stops activities by rogue security software, also known as FakeAV. The agent also uses advanced cleanup rules to proactively detect and stop applications that exhibit FakeAV behavior.  
  **Note**: While providing proactive protection, advanced cleanup also results in a high number of false-positives. |

### Spyware/Grayware Approved List

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

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

**Scan Actions**

The following are the actions that Security Agents can perform against viruses/malware:

**TABLE 7-1. Virus/Malware Scan Actions**

<table>
<thead>
<tr>
<th><strong>ACTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Deletes the infected file.</td>
</tr>
</tbody>
</table>
| Quarantine | Renames and then moves the infected file to a temporary quarantine directory on the client.  
   The Security Agents then sends quarantined files to the designated quarantine directory, which is on the Security Server by default.  
   The Security Agent encrypts quarantined files sent to this directory.  
   If you need to restore any of the quarantined files, use the VSEncrypt tool. For information on using this tool, see *Restoring Encrypted Files on page 14-9*. |
| Clean      | Cleans the infected file before allowing full access to the file.  
   If the file is uncleanable, the Security Agent performs a second action, which can be one of the following actions: Quarantine, Delete, Rename, and Pass.  
   This action can be performed on all types of malware except probable virus/malware. |

---

**Note**

Some files are uncleanable. For details, see *Uncleanable Files on page D-26*. |
### Managing Scans

**Rename**
Changes the infected file’s extension to "vir". Users cannot open the renamed file initially, but can do so if they associate the file with a certain application.

The virus/malware may execute when opening the renamed infected file.

**Pass**
Only performed during Manual Scan and Scheduled Scan. The Security Agent cannot use this scan action during Real-time Scan because performing no action when an attempt to open or execute an infected file is detected will allow virus/malware to execute. All the other scan actions can be used during Real-time Scan.

**Deny Access**
Only performed during Real-time Scan. When the Security Agent detects an attempt to open or execute an infected file, it immediately blocks the operation.

Users can manually delete the infected file.

The scan action the Security Agent performs depends on the scan type that detected the spyware/grayware. While specific actions can be configured for each virus/malware type, only one action can be configured for all types of spyware/grayware. For example, when the Security Agent detects any type of spyware/grayware during Manual Scan (scan type), it cleans (action) the affected system resources.

The following are the actions the Security Agent can perform against spyware/grayware:

**Table 7-2. Spyware/Grayware Scan Actions**

<table>
<thead>
<tr>
<th><strong>Action</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean</td>
<td>Terminates processes or delete registries, files, cookies, and shortcuts.</td>
</tr>
<tr>
<td>Pass</td>
<td>Performs no action on detected spyware/grayware components but records the spyware/grayware detection in the logs. This action can only be performed during Manual Scan and Scheduled Scan. During Real-time Scan, the action is &quot;Deny Access&quot;. The Security Agent will not perform any action if the detected spyware/grayware is included in the approved list.</td>
</tr>
<tr>
<td>Deny Access</td>
<td>Denies access (copy, open) to the detected spyware/grayware components. This action can only be performed during Real-time Scan. During Manual Scan and Scheduled Scan, the action is &quot;Pass&quot;.</td>
</tr>
</tbody>
</table>
ActiveAction

Different types of virus/malware require different scan actions. Customizing scan actions requires knowledge about virus/malware and can be a tedious task. Worry-Free Business Security uses ActiveAction to counter these issues.

ActiveAction is a set of pre-configured scan actions for viruses/malware. 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:

- ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- Virus writers constantly change the way virus/malware attack computers. ActiveAction settings are updated to protect against the latest threats and the latest methods of virus/malware attacks.

The following table illustrates how ActiveAction handles each type of virus/malware:

<table>
<thead>
<tr>
<th>VIRUS/MALWARE TYPE</th>
<th>REAL-TIME SCAN</th>
<th>MANUAL SCAN/SCHEDULED SCAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FIRST ACTION</td>
<td>SECOND ACTION</td>
</tr>
<tr>
<td>Joke program</td>
<td>Quarantine</td>
<td>Delete</td>
</tr>
<tr>
<td>Trojan horse program/Worms</td>
<td>Quarantine</td>
<td>Delete</td>
</tr>
<tr>
<td>Packer</td>
<td>Quarantine</td>
<td>N/A</td>
</tr>
<tr>
<td>Probable virus/malware</td>
<td>Deny Access or user-configured action</td>
<td>N/A</td>
</tr>
<tr>
<td>Virus</td>
<td>Clean</td>
<td>Quarantine</td>
</tr>
<tr>
<td>Test virus</td>
<td>Deny Access</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Managing Scans

<table>
<thead>
<tr>
<th>VIRUS/MALWARE TYPE</th>
<th>REAL-TIME SCAN</th>
<th>MANUAL SCAN/SCHEDULED SCAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FIRST ACTION</td>
<td>SECOND ACTION</td>
</tr>
<tr>
<td>Other malware</td>
<td>Clean</td>
<td>Quarantine</td>
</tr>
</tbody>
</table>

Notes and Reminders:

- For probable virus/malware, the default action is "Deny Access" during Real-time Scan and "Pass" during Manual Scan and Scheduled Scan. If these are not your preferred actions, you can change them to Quarantine, Delete, or Rename.

- Some files are uncleanable. For details, see Uncleanable Files on page D-26.

- ActiveAction is not available for spyware/grayware scan.

Advanced Settings (Scan Actions)

<table>
<thead>
<tr>
<th>SCAN TYPE</th>
<th>OPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time Scan, Scheduled Scan</td>
<td>Display an alert message on the desktop or server when a virus/spyware is detected</td>
</tr>
<tr>
<td>Real-time Scan, Scheduled Scan</td>
<td>Display an alert message on the desktop or server when a probable virus/spyware is detected</td>
</tr>
<tr>
<td>Manual Scan, Real-time Scan, Scheduled Scan</td>
<td>Run cleanup when probable virus/malware is detected: Only available if you choose ActiveAction and customized the action for probable virus/malware.</td>
</tr>
</tbody>
</table>

Scan Targets and Actions for Messaging Security Agents

Configure the following settings for each scan type (Manual Scan, Scheduled Scan, and Real-time Scan):

Target Tab
- Scan Targets
• Additional Threat Scan Settings
• Scan Exclusions

**Action Tab**

• Scan Actions/ActiveAction
• Notifications
• Advanced Settings

**Scan Targets**

Select scan targets:

• **All attachment files**: Only encrypted or password-protected files are excluded.

---

**Note**
This option provides the maximum security possible. However, scanning every file requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files the agent includes in the scan.

---

• **IntelliScan**: Scans files based on true-file type. See *IntelliScan on page D-2*.

• **Specific file types**: WFBS will scan files of the selected types and with the selected extensions. Separate multiple entries with semicolons (;).

Select other options:

• **Enable IntelliTrap**: IntelliTrap detects malicious code, such as bots, in compressed files. See *IntelliTrap on page D-2*.

• **Scan message body**: Scans the body of an email message that could contain embedded threats.

**Additional Threat Scan Settings**

Select other threats the agent should scan. For details about these threats, see *Understanding Threats on page 1-8*.

Select additional options:
• **Backup infected file before cleaning**: WFBS makes a backup of the threat before cleaning. The backed-up file is encrypted and stored in the following directory on the client:

\<Messaging Security Agent installation folder>\storage\backup

You can change the directory in the **Advanced Options** section, **Backup Setting** subsection.

To decrypt the file, see *Restoring Encrypted Files on page 14-9*.

• **Do not clean infected compressed files to optimize performance**

**Scan Exclusions**

Under the **Target** tab, go to the **Exclusions** section and select from the following criteria that the agent will use when excluding email messages from scans:

• **Message body size exceeds**: The Messaging Security Agent only scans email messages when the size of the body of the message is smaller or equal to the specified amount.

• **Attachment size exceeds**: The Messaging Security Agent only scans email messages when the size of the attachment file is smaller than or equal to the specified amount.

```
Tip
Trend Micro recommends a 30 MB limit.
```

• **Decompressed file count exceeds**: When the amount of decompressed files within the compressed file exceeds this number, then the Messaging Security Agent only scans files up to the limit set by this option.

• **Size of decompressed file exceeds**: The Messaging Security Agent only scans compressed files that are smaller or equal to this size after decompression.

• **Number of layers of compression exceeds**: The Messaging Security Agent only scans compressed files that have less than or equal to the specified layers of compression. For example, if you set the limit to 5 layers of compression, then the
Messaging Security Agent will scan the first 5 layers of compressed files, but not scan files compressed to 6 or more layers.

- **Size of decompressed file is “x” times the size of compressed file:** The Messaging Security Agent only scans compressed files when the ratio of the size of the decompressed file compared to the size of the compressed file is less than this number. This function prevents the Messaging Security Agent from scanning a compressed file that might cause a Denial of Service (DoS) attack. A DoS attack happens when a mail server’s resources are overwhelmed by unnecessary tasks. Preventing the Messaging Security Agent from scanning files that decompress into very large files helps prevent this problem from happening.

Example: For the table below, the value typed for the “x” value is 100.

<table>
<thead>
<tr>
<th>FILE SIZE (NOT COMPRESSED)</th>
<th>FILE SIZE (NOT COMPRESSED)</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 KB</td>
<td>10 KB (ratio is 50:1)</td>
<td>Scanned</td>
</tr>
<tr>
<td>1000 KB</td>
<td>10 KB (ratio is 100:1)</td>
<td>Scanned</td>
</tr>
<tr>
<td>1001 KB</td>
<td>10 KB (ratio exceeds 100:1)</td>
<td>Not scanned *</td>
</tr>
<tr>
<td>2000 KB</td>
<td>10 KB (ratio is 200:1)</td>
<td>Not scanned *</td>
</tr>
</tbody>
</table>

* The Messaging Security Agent takes the action you configure for excluded files.

**Scan 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 7-4. Messaging Security Agent Customized Actions

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean</td>
<td>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 Scan or Scheduled Scan, the Messaging Security Agent updates the Information Store and replaces the file with the cleaned one.</td>
</tr>
<tr>
<td>Replace with text/file</td>
<td>Deletes the infected/filtered 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. For Content Filtering and Data Loss Prevention, you can replace text only in the body or attachment fields (and not From, To, Cc, or Subject).</td>
</tr>
<tr>
<td>Quarantine entire message</td>
<td>(Real-time Scan only) Quarantines only the infected content to the quarantine directory and the recipient receives the message without this content. For Content Filtering, Data Loss Prevention, and Attachment Blocking, moves the entire message to the quarantine directory.</td>
</tr>
<tr>
<td>Quarantine message part</td>
<td>(Real-time Scan only) Quarantines only the infected or filtered content to the quarantine directory and the recipient receives the message without this content.</td>
</tr>
<tr>
<td>Delete entire message</td>
<td>(Real-time Scan only) Deletes the entire email message. The original recipient will not receive the message.</td>
</tr>
<tr>
<td>Pass</td>
<td>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. For Content Filtering, delivers the message as-is.</td>
</tr>
<tr>
<td><strong>ACTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Archive</td>
<td>Moves the message to the archive directory and delivers the message to the original recipient.</td>
</tr>
<tr>
<td>Quarantine message to server-side spam folder</td>
<td>Sends the entire message to the Security Server for quarantine.</td>
</tr>
<tr>
<td>Quarantine message to user's spam folder</td>
<td>Sends the entire message to the user’s spam folder for quarantine. The folder is located on the server-side of the Information Store.</td>
</tr>
<tr>
<td>Tag and deliver</td>
<td>Adds a tag to the header information of the email message that identifies it as spam and then delivers it to the intended recipient.</td>
</tr>
</tbody>
</table>

In addition to these actions, you can also configure the following:

- **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.

- **Do this when clean is unsuccessful**: Set the secondary action for unsuccessful cleaning attempts. Select from Replace with Text/File, Delete Entire message, Pass, or Quarantine the message part.

**ActiveAction**

The following table illustrates how ActiveAction handles each type of virus/malware:

**Table 7-5. Trend Micro Recommended Scan Actions Against Viruses and Malware**

<table>
<thead>
<tr>
<th>VIRUS/MALWARE TYPE</th>
<th>REAL-TIME SCAN</th>
<th>MANUAL SCAN/SCHEDULED SCAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FIRST ACTION</td>
<td>SECOND ACTION</td>
</tr>
<tr>
<td>Virus</td>
<td>Clean</td>
<td>Delete entire message</td>
</tr>
<tr>
<td>Trojan horse program/Worms</td>
<td>Replace with text/file</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Scan Action Notifications

Select **Notify recipients** to set the Messaging Security Agent to notify the intended recipients when taking action against a specific email message. For various reasons, you may want to avoid notifying external mail recipients that a message containing sensitive information was blocked. Select **Do not notify external recipients** to only send notifications to internal mail recipients. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

You can also disable sending notifications to spoofing senders’ external recipients.

<table>
<thead>
<tr>
<th>VIRUS/MALWARE TYPE</th>
<th>REAL-TIME SCAN</th>
<th>MANUAL SCAN/SCHEDULED SCAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FIRST ACTION</td>
<td>SECOND ACTION</td>
</tr>
<tr>
<td>Packer</td>
<td>Quarantine message part</td>
<td>N/A</td>
</tr>
<tr>
<td>Other malicious code</td>
<td>Clean</td>
<td>Delete entire message</td>
</tr>
<tr>
<td>Additional threats</td>
<td>Quarantine message part</td>
<td>N/A</td>
</tr>
<tr>
<td>Mass-mailing behavior</td>
<td>Delete entire message</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Select **Notify recipients** to set the Messaging Security Agent to notify the intended recipients when taking action against a specific email message. For various reasons, you may want to avoid notifying external mail recipients that a message containing sensitive information was blocked. Select **Do not notify external recipients** to only send notifications to internal mail recipients. Define internal addresses from **Operations > Notification Settings > Internal Mail Definition**.

You can also disable sending notifications to spoofing senders’ external recipients.
## Advanced Settings (Scan Actions)

<table>
<thead>
<tr>
<th>SETTINGS</th>
<th>DETAILS</th>
</tr>
</thead>
</table>
| Macros         | Macro viruses are application-specific viruses that infect macro utilities that accompany applications. Advanced macro scanning uses heuristic scanning to detect macro viruses or strip all detected macro codes. 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. The Messaging Security Agent takes action against malicious macro code depending on the action that you configure. • **Heuristic level**  
  • Level 1 uses the most specific criteria, but detects the least macro codes.  
  • Level 4 detects the most macro codes, but uses the least specific criteria and may falsely identify safe macro code as harboring malicious macro code.  
  
  **Tip**  
  Trend Micro recommends a heuristic scan level of 2. This level provides a high detection level for unknown macro viruses, fast scanning speed, and it uses only the necessary rules to check for macro virus strings. Level 2 also has a low level of incorrectly identifying malicious code in safe macro code.  
  • **Delete all macros detected by advanced macro scan**: Strip all of the macro codes detected on scanned files  
| Unscannable Message Parts | Set the action and notification condition for encrypted and/or password-protected files. For the action, select from Replace with text/file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part. |
### Settings Details

<table>
<thead>
<tr>
<th>Settings</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excluded Message Parts</td>
<td>Set the action and notification condition for parts of messages that have been excluded. For the action, select from Replace with text/file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part.</td>
</tr>
<tr>
<td>Backup Setting</td>
<td>The location to save the backup of infected files before the agent cleaned them.</td>
</tr>
<tr>
<td>Replacement Settings</td>
<td>Configure the text and file for replacement text. If the action is <strong>replace with text/file</strong>, WFBS will replace the threat with this text string and file.</td>
</tr>
</tbody>
</table>
Chapter 8

Managing Updates

This chapter describes Worry-Free Business Security components and update procedures.
Update Overview

All component updates originate from the Trend Micro ActiveUpdate server. When updates are available, the Security Server downloads the updated components and then distributes them to Security Agents and Messaging Security Agents (Advanced only).

If a Security Server manages a large number of Security Agents, updating may utilize a significant amount of server computer resources, affecting the server’s stability and performance. To address this issue, Worry-Free Business Security has an Update Agent feature that allows certain Security Agents to share the task of distributing updates to other Security Agents.

The following table describes the component update options for the Security Server and agents, and recommendations on when to use them:

**Table 8-1. Update Options**

<table>
<thead>
<tr>
<th><strong>Update Sequence</strong></th>
<th><strong>Description</strong></th>
<th><strong>Recommendation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ActiveUpdate Server or custom update source</td>
<td>The Trend Micro Security Server receives updated components from the ActiveUpdate server or custom update source and then deploys them directly to agents (Security Agents and Messaging Security Agents).</td>
<td>Use this method if there are no low-bandwidth sections between the Security Server and agents.</td>
</tr>
<tr>
<td>2. Security Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Agents</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Update Sequence

<table>
<thead>
<tr>
<th><strong>Update Sequence</strong></th>
<th><strong>Description</strong></th>
<th><strong>Recommendation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ActiveUpdate Server or custom update source</td>
<td>The Trend Micro Security Server receives updated components from the ActiveUpdate server or custom update source and then deploys them directly to:   • Update Agents   • Messaging Security Agents   • Security Agents without Update Agents</td>
<td>If there are low-bandwidth sections between the Security Server and Security Agents, use this method to balance the traffic load on the network.</td>
</tr>
<tr>
<td>2. Security Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Update Agents, Messaging Security Agents, Security Agents without Update Agents</td>
<td>The Update Agents then deploy the components to their respective Security Agents. If these Security Agents are unable to update, they update directly from the Security Server.</td>
<td></td>
</tr>
<tr>
<td>4. All other Security Agents</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Updatable Components

Worry-Free Business Security makes use of components to keep clients protected from the latest threats. Keep these components up-to-date by running manual or scheduled updates.

---

**Note**

Messaging Security Agents never update directly from the ActiveUpdate server. If all sources are unavailable, the Messaging Security Agent quits the update process.

This mechanism is provided only as a last resort.
View the status of Outbreak Defense, Antivirus, Anti-spyware, and Network Virus components from the Live Status screen. If Worry-Free Business Security is protecting Microsoft Exchange servers (Advanced only), you can also view the status of Anti-spam components. WFBS can send a notification to Administrators when component updates is necessary.

The following tables list the components downloaded by the Security Server from the ActiveUpdate server:

**Messaging Components (Advanced only)**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging Security Agent Anti-spam Pattern</td>
<td>Messaging Security Agents</td>
<td>The Anti-spam Pattern identifies the latest spam in email messages and email attachments.</td>
</tr>
<tr>
<td>Messaging Security Agent Scan Engine 32/64-bit</td>
<td>Messaging Security Agents</td>
<td>The Scan Engine detects Internet worms, mass-mailers, Trojans, phishing sites, spyware, network exploits and viruses in email messages and email attachments.</td>
</tr>
<tr>
<td>Messaging Security Agent URL Filtering Engine 32/64-bit</td>
<td>Messaging Security Agents</td>
<td>The URL Filtering Engine facilitates communication between WFBS and the Trend Micro URL Filtering Service. The URL Filtering Service is a system that rates URLs and provides rating information to WFBS.</td>
</tr>
</tbody>
</table>
## Antivirus and Smart Scan

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Virus Scan Engine 32/64-bit | Security Agents  | At the heart of all Trend Micro products lies the scan engine, which was originally developed in response to early file-based computer viruses. The scan engine today is exceptionally sophisticated and capable of detecting different types of viruses and malware. The scan engine also detects controlled viruses that are developed and used for research. Rather than scanning every byte of every file, the engine and pattern file work together to identify the following:  
  - Tell-tale characteristics of the virus code  
  - The precise location within a file where the virus resides |
<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Scan Pattern</td>
<td>Not distributed to Security Agents. This pattern stays in the Security Server and is used when responding to scan queries received from Security Agents.</td>
<td>When in smart scan mode, Security Agents use two lightweight patterns that work together to provide the same protection provided by conventional anti-malware and anti-spyware patterns. The <strong>Smart Scan Pattern</strong> contains majority of the pattern definitions. The <strong>Smart Scan Agent Pattern</strong> contains all the other pattern definitions not found on the Smart Scan Pattern. The Security Agent scans the client for security threats using the <strong>Smart Scan Agent Pattern</strong>. A Security Agent that cannot determine the risk of the file during the scan verifies the risk by sending a scan query to the Scan Server, a service hosted on the Security Server. The Scan Server verifies the risk using the <strong>Smart Scan Pattern</strong>. The Security Agent &quot;caches&quot; the scan query result provided by the Scan Server to improve the scan performance.</td>
</tr>
<tr>
<td>Smart Scan Agent Pattern</td>
<td>Security Agents using smart scan</td>
<td></td>
</tr>
<tr>
<td>Virus Pattern</td>
<td>Security Agents using conventional scan</td>
<td>The Virus Pattern contains information that helps Security Agents identify the latest virus/malware and mixed threat attacks. Trend Micro creates and releases new versions of the Virus Pattern several times a week, and any time after the discovery of a particularly damaging virus/malware.</td>
</tr>
<tr>
<td>IntelliTrap Pattern</td>
<td>Security Agents</td>
<td>The IntelliTrap Pattern detects real-time compression files packed as executable files. For details, see <em>IntelliTrap on page D-2</em>.</td>
</tr>
<tr>
<td>IntelliTrap Exception Pattern</td>
<td>Security Agents</td>
<td>The IntelliTrap Exception Pattern contains a list of &quot;approved&quot; compression files.</td>
</tr>
</tbody>
</table>
Managing Updates

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage Cleanup Engine 32/64-bit</td>
<td>Security Agents</td>
<td>The Damage Cleanup Engine scans for and removes Trojans and Trojan processes.</td>
</tr>
<tr>
<td>Damage Cleanup Template</td>
<td>Security Agents</td>
<td>The Damage Cleanup Template is used by the Damage Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.</td>
</tr>
</tbody>
</table>

Anti-spyware

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware/Grayware Scan Engine v.6 32/64-bit</td>
<td>Security Agents</td>
<td>The Spyware Scan Engine scans for and performs the appropriate scan action on spyware/grayware.</td>
</tr>
<tr>
<td>Spyware/Grayware Pattern v.6</td>
<td>Security Agents</td>
<td>The Spyware Pattern identifies spyware/grayware in files and programs, modules in memory, Windows registry and URL shortcuts.</td>
</tr>
<tr>
<td>Spyware/Grayware Pattern</td>
<td>Security Agents</td>
<td></td>
</tr>
</tbody>
</table>

Network Virus

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Pattern</td>
<td>Security Agents</td>
<td>Like the Virus Pattern, the Firewall Pattern helps agents identify virus signatures, unique patterns of bits and bytes that signal the presence of a network virus.</td>
</tr>
</tbody>
</table>

Behavior Monitoring and Device Control

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior Monitoring Detection Pattern 32/64-bit</td>
<td>Security Agents</td>
<td>This pattern contains the rules for detecting suspicious threat behavior.</td>
</tr>
</tbody>
</table>
## Component

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior Monitoring Core Driver 32/64-bit</td>
<td>Security Agents</td>
<td>This kernel mode driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.</td>
</tr>
</tbody>
</table>
| Behavior Monitoring Core Service 32/64-bit | Security Agents | This user mode service has the following functions:  
• Provides rootkit detection  
• Regulates access to external devices  
• Protects files, registry keys, and services |
| Behavior Monitoring Configuration Pattern | Security Agents | The Behavior Monitoring Driver uses this pattern to identify normal system events and exclude them from policy enforcement. |
| Digital Signature Pattern | Security Agents | This pattern contains a list of valid digital signatures that are used by the Behavior Monitoring Core Service to determine whether a program responsible for a system event is safe. |
| Policy Enforcement Pattern | Security Agents | The Behavior Monitoring Core Service checks system events against the policies in this pattern. |

## Outbreak Defense

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DISTRIBUTED TO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Assessment Pattern 32/64-bit</td>
<td>Security Agents</td>
<td>A file that includes the database for all vulnerabilities. The Vulnerability Assessment Pattern provides instructions for the scan engine to scan for known vulnerabilities.</td>
</tr>
</tbody>
</table>
Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops the following to address issues, enhance product performance, or add new features:

- **Hot Fix on page D-2**
- **Patch on page D-9**
- **Security Patch on page D-25**
- **Service Pack on page D-25**

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

http://www.trendmicro.com/download

All releases include a readme file that contains installation, deployment, and configuration information. Read the readme file carefully before performing installation.

Security Server Updates

**Automatic Updates**

The Security Server automatically performs the following updates:

- Immediately after installing the Security Server, it updates from the Trend Micro ActiveUpdate server.
- Whenever the Security Server starts, it updates the components and the Outbreak Defense policy.
- By default, scheduled updates run every hour (the update frequency can be changed from the web console).

**Manual Updates**

You can run manual updates from the web console if an update is urgent.


Server Update Reminders and Tips

- After an update, the Security Server automatically distributes the component updates to agents. For details on the components distributed to agents, see Updatable Components on page 8-3.

- A pure IPv6 Security Server cannot perform the following tasks:
  - Obtain updates directly from the Trend Micro ActiveUpdate server or a pure IPv4 custom update source.
  - Distribute updates directly to pure IPv4 agents.

Similarly, a pure IPv4 Security Server cannot obtain updates directly from a pure IPv6 custom update source and distribute updates to pure IPv6 agents.

In these situations, a dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Security Server to obtain and distribute updates.

- If you use a proxy server to connect to the Internet, set the correct proxy settings in Preferences > Global Settings > Proxy tab to download updates successfully.

Component Duplication

Trend Micro releases pattern files regularly to keep client protection current. Since pattern file updates are available regularly, the Security Server uses a mechanism called component duplication that allows faster downloads of pattern files.

When the latest version of a full pattern file is available for download from the Trend Micro ActiveUpdate server, incremental patterns also become available. Incremental patterns are smaller versions of the full pattern file that account for the difference between the latest and previous full pattern file versions. For example, if the latest version is 175, incremental pattern v_173.175 contains signatures in version 175 not found in version 173 (version 173 is the previous full pattern version since pattern numbers are released in increments of 2). Incremental pattern v_171.175 contains signatures in version 175 not found in version 171.

To reduce network traffic generated when downloading the latest pattern, the Security Server performs component duplication, a component update method where the server downloads only incremental patterns. To take advantage of component duplication, be sure that the Security Server is updated regularly. Otherwise, the server will be forced to download the full pattern file.
Component duplication applies to the following components:

- Virus Pattern
- Smart Scan Agent Pattern
- Damage Cleanup Template
- IntelliTrap Exception Pattern
- Spyware Pattern

Configuring the Security Server Update Source

Before you begin

By default, the Security Server obtains updates from the Trend Micro ActiveUpdate server. Specify a custom update source if the Security Server is unable to reach the ActiveUpdate server directly.

- If the source is the Trend Micro ActiveUpdate Server, ensure that the Security Server has Internet connection and, if you are using a proxy server, test if Internet connection can be established using the proxy settings. For details, see Configuring Internet Proxy Settings on page 11-3.

- If the source is a custom update source (Intranet location containing a copy of the current file or Alternate update source), set up the appropriate environment and update resources for this update source. Also ensure that there is a functional connection between the Security Server and this update source. If you need assistance setting up an update source, contact your support provider.

- A pure IPv6 Security Server cannot update directly from the Trend Micro ActiveUpdate server or any pure IPv4 custom update source. Similarly, a pure IPv4 Security Server cannot update directly from pure IPv6 custom update sources. A dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the Security Server to connect to the update sources.

Procedure

1. Navigate to Updates > Source.
2. On the Server tab, select an update source.
   • Trend Micro ActiveUpdate Server
   • Intranet location containing a copy of the current file: Type the Universal Naming Convention (UNC) path to the source, such as \Web\ActiveUpdate. Also specify the logon credentials (user name and password) that the Security Server will use to connect to this source.
   • Alternate update source: Type the URL to this source. Be sure that the target HTTP virtual directory (Web share) is available to the Security Server.

3. Click Save.

---

**Updating the Security Server Manually**

Manually update the components on the Security Server after installing or upgrading the server and whenever there is an outbreak.

---

**Procedure**

1. Start a manual update in two ways:
   • Navigate to Updates > Manual.
   • Navigate to Live Status, go to System Status > Component Updates, and click Update Now.

2. Select the components to update.

   For details about components, see Updatable Components on page 8-3.

3. Click Update.

   A new screen displays, showing the update status. If the update is successful, the Security Server automatically distributes the updated components to agents.
Configuring Scheduled Updates for the Security Server

Configure the Security Server to regularly check its update source and automatically download any available updates. Using scheduled update is an easy and effective way of ensuring that protection against threats is always current.

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.

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

**Procedure**

1. Navigate to Updates > Scheduled.
2. Select the components to update.
   
   For details about components, see *Updatable Components on page 8-3*.
3. Click the Schedule tab and then specify the update schedule.

   - **Conventional scan updates** include all components, except the Smart Scan Pattern and Smart Scan Agent Pattern. Choose between daily, weekly, and monthly updates, and then specify a value for *Update for a period of*, which is the number of hours during which the Security Server will perform the update. The Security Server updates at any given time during this time period.

   **Note**
   For monthly scheduled updates (not recommended), if you select 31, 30, or 29 days and a month has less than the number of days, the update will not run that month.

   - **Smart scan updates** include only the Smart Scan Pattern and Smart Scan Agent Pattern. If none of your agents use smart scan, disregard this item.
4. Click Save.

Rolling Back Components

Rollback refers to reverting to the previous version of the Virus Pattern, Smart Scan Agent Pattern, and Virus Scan Engine. If these components do not function properly, roll them back to their previous versions. The Security Server retains the current and the previous versions of the Virus Scan Engine, and the last three versions of the Virus Pattern and Smart Scan Agent Pattern.

Note

Only the above-mentioned components can be rolled back.

Worry-Free Business Security uses different scan engines for agents running 32-bit and 64-bit platforms. You need to roll back these scan engines separately. The rollback procedure for all types of scan engines is the same.

Procedure

1. Navigate to Updates > Rollback.

2. Click Synchronize for a specific component to notify agents to synchronize their component versions with the version on the server.

3. Click Rollback for a specific component to roll back that component on both the Security Server and agents.

Security Agent and Messaging Security Agent Updates

Automatic Updates

Security Agents and Messaging Security Agents (Advanced only) automatically perform the following updates:
Managing Updates

• Immediately after installation, the agents update from the Security Server.

• Each time the Security Server completes an update, it automatically pushes the updates to agents.

• Each time an Update Agent completes an update, it automatically pushes the updates to the respective Security Agents.

• By default, scheduled updates run:
  • Every 8 hours on In Office Security Agents
  • Every 2 hours on Out of Office Security Agents

• By default, Messaging Security Agents run a scheduled update every 24 hours at 12:00 AM.

Manual Updates

Run a manual update from the web console if an update is urgent. Navigate to Live Status, go to System Status > Component Updates, and click Deploy Now.

Agent Update Reminders and Tips

• Security Agents update from the Security Server, Update Agents, or the Trend Micro ActiveUpdate server.
  
Messaging Security Agents update only from the Security Server.

For details on the update process, see Update Overview on page 8-2.

• A pure IPv6 agent cannot obtain updates directly from a pure IPv4 Security Server/Update Agent and the Trend Micro ActiveUpdate server.

Similarly, a pure IPv4 agent cannot obtain updates directly from a pure IPv6 Security Server/Update Agent.

In these situations, a dual-stack proxy server that can convert IP addresses, such as DeleGate, is required to allow the agent to obtain updates.

• For details on the components that agents update, see Updatable Components on page 8-3.

• In addition to the components, agents also receive updated configuration files when updating from the Security Server. Agents need the configuration files to
apply new settings. Each time you modify agent settings through the web console, the configuration files change.

**Update Agents**

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

If you identify sections of your network between clients and the Trend Micro Security Server as “low-bandwidth” or “heavy traffic”, you can specify Security Agents to act as Update Agents. Update Agents reduce network bandwidth consumption by eliminating the need for all Security Agents to access the Security Server for component updates. If your network is segmented by location and the network link between segments frequently experiences a heavy traffic load, Trend Micro recommends allowing at least one Security Agent on each segment to act as an Update Agent.

The Update Agent update process can be described as follows:

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

2. The Update Agents download the updated components from the Security Server.
3. The Security Server then notifies the Security Agents that updated components are available.

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

Configuring Update Agents

Procedure

1. Navigate to Updates > Source.

2. Click the Update Agents tab.

3. Perform the following tasks:
## Assign Security Agents as Update Agents

<table>
<thead>
<tr>
<th><strong>Task</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
</table>
| **Assign Security Agents as Update Agents** | **a.** In the **Assign Update Agent(s)** section, click **Add**.  
A new screen opens.  

**b.** From the list box, select one or more agents to act as Update Agents.  

**c.** Click **Save**.  
The screen closes.  

**d.** Back in the **Assign Update Agent(s)** section, select **Update Agents always update directly from the Security Server only** if you want Update Agents to always download updated components from the Security Server instead of another Update Agent. |
### Configure Security Agents to update from Update Agents

<table>
<thead>
<tr>
<th>TASK</th>
<th>STEPS</th>
</tr>
</thead>
</table>
| a. In the **Alternative Update Sources** section, select **Enable alternative update sources for Security Agents and Update Agents**.  

  **Note**  
  Disabling this option prevents Security Agents from updating from Update Agents, effectively switching their update source back to the Security Server. |
| b. Click **Add**.  
  A new screen opens.  
  c. Type the IP addresses of the Security Agents that will update from an Update Agent.  
  • Type an IPv4 address range.  
    To specify a single Security Agent, enter the Security Agent’s IP address in both the **from** and **to** fields.  
  • For IPv6, type an IP prefix and length.  
  d. Select an Update Agent from the drop-down list.  
  If the drop-down list is not available, no Update Agents have been configured.  
  e. Click **Save**.  
  The screen closes.  
  f. Define more IP ranges as necessary. If you have defined several IP ranges, you can use the **Reorder** option to set the IP range priority. When the Security Server notifies Security Agents that updates are available, they scan the IP Range list to identify their correct update source. The Security Agent scans the first item on the list and continues down the list until it identifies its correct update source.  

  **Tip**  
  Define several Update Agents for the same IP range as a failover measure. This means that if the Security Agents are unable to update from an Update Agent, they will try other Update Agents. To do this, create at least two (2) entries with the same IP range and assign each entry a different Update Agent. |
Managing Updates

### To remove an Update Agent and unassign all Security Agents assigned to it

1. Go to the **Assign Update Agent(s)** section, select the check box corresponding to the Update Agent’s Computer Name, and click **Remove**.

   - **Steps**: To remove an Update Agent and unassign all Security Agents assigned to it, go to the **Assign Update Agent(s)** section, select the check box corresponding to the Update Agent’s Computer Name, and click **Remove**.
   - **Explanation**: This action will not remove the Security Agents’ IP address range in the **Alternative Update Sources** section and will only cause the “orphaned” Security Agents to switch their update source back to the Security Server. If you have another Update Agent, you can assign it to the orphaned Security Agents.

### To unassign Security Agents from Update Agents

2. Go to the **Alternative Update Sources** section, select the check box corresponding to the Security Agents’ IP address range, and click **Remove**.

   - **Steps**: If you no longer want Security Agents belonging to an IP address range to update from an Update Agent, go to the **Alternative Update Sources** section, select the check box corresponding to the Security Agents’ IP address range, and click **Remove**.

4. **Click Save.**
Chapter 9

Managing Notifications

This chapter explains how to use the different notification options.
Notifications

Administrators can receive notifications whenever there are abnormal events on the network. Worry-Free Business Security can send notifications using email, SNMP, or Windows event logs.

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

Threat Events

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

- **Smart Scan**: Clients configured for Smart Scan cannot connect to the Smart Scan server or the server is not available.

- **Component update**: Last time components updated exceeds a certain number of days or updated components not deployed to Agents quick enough.

- **Unusual system events**: Remaining disk space on any of the clients running Windows Server operating system is less than the configured amount, reaching dangerously low levels.

License Events

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

**Configuring Events for Notifications**

Configuring notifications involves two steps. First, select the events for which you need notifications and second, configure the methods of delivery.

Worry-Free Business Security offers three methods for delivery:

- Email notifications
- SNMP notifications
- Windows Event log

**Procedure**

1. Navigate to **Preferences > Notifications**.

2. From the **Events** tab, update the following as required:

   - **Email**: Select the check box to receive notifications for that event.
   - **Alert Threshold**: Configure the threshold and/or time period for the event.
• **Event name**: Click an event name to modify the content of the notification for that event. You can add token variables to the content. For details, see *Token Variables on page 9-4*.

3. Click the **Settings** tab and update the following as required:

   • **Email Notification**: Set the email addresses of the sender and recipients. For recipients, 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**

4. Click **Save**.

---

### Token Variables

Use token variables to customize the subject line and the message body of event notifications.

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

The following tokens represent threat events detected on desktops/servers and Microsoft Exchange servers.

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>{$CSM_SERVERNAME}</td>
<td>The name of the Security Server that manages the agents</td>
</tr>
<tr>
<td>VARIABLE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>%CV</td>
<td>Number of incidents</td>
</tr>
<tr>
<td>%CU</td>
<td>The time unit (minutes, hours)</td>
</tr>
<tr>
<td>%CT</td>
<td>Number of %CU</td>
</tr>
<tr>
<td>%CP</td>
<td>Percentage of total email messages that is spam</td>
</tr>
</tbody>
</table>

The following is an example notification:

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

Refer to the Live Status screen on the Security Server for further instructions.
Chapter 10

Using Outbreak Defense

This chapter explains the Worry-Free Business Security Outbreak Defense strategy, how to configure Outbreak Defense, and how to use it to protect networks and clients.
Outbreak Defense Strategy

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

WFBS initiates Outbreak Defense in response to instructions that it receives in the Outbreak Prevention Policy (OPP). The Trend Micro Outbreak Prevention Policy are content filtering rules 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.

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. This may interrupt the normal functions of your network by measures like blocked ports and inaccessible directories. By customizing Outbreak Defense settings for your clients and network you can avoid unexpected consequences from the Outbreak Prevention Policy being enacted during Outbreak Defense.

As part of Outbreak Defense, Trend Micro may send out alerts and other information in response to threat conditions. For example:

**Red Alerts**

Several business units have reported a rapidly spreading virus/malware. As a response, Trend Micro triggers its 45-minute Red Alert solution process, which releases preventive solutions and scan patterns, sending out relevant notifications and any fix tools, along with vulnerability and threat information.

**Yellow Alerts**

Infection reports have been received from several business units; support calls confirm scattered instances. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download.

In case of an email-spreading virus/malware (Advanced only), Outbreak Prevention Policies are automatically sent to block attachments on servers equipped with the product functionality.
Outbreak Life Cycle

Outbreak Defense strategy is based on the idea of an Internet-wide outbreak life cycle.

The life cycle of an outbreak is divided into three stages: **Threat Prevention**, **Threat Protection**, and **Threat Cleanup**. Trend Micro responds to each stage with a defense strategy called Outbreak Defense.

**Table 10-1. Outbreak Defense Response to the Outbreak Life Cycle Stages**

<table>
<thead>
<tr>
<th>Outbreak Stage</th>
<th>Outbreak Defense Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Threat Prevention&lt;br&gt;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.</td>
</tr>
<tr>
<td>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.</td>
<td>Threat Protection&lt;br&gt;Outbreak Defense protects at-risk computers by notifying them to download the latest components and patches.</td>
</tr>
<tr>
<td>In the third and final stage of an outbreak, the threat subsides with fewer reported incidents.</td>
<td>Threat Cleanup&lt;br&gt;Outbreak Defense repairs damage by running Cleanup services. Other scans provide information that Administrators can use to prepare for future threats.</td>
</tr>
</tbody>
</table>

Outbreak Defense Actions

The Outbreak Defense strategy manages outbreaks at every stage of the outbreak life cycle. Based on the Outbreak Prevention Policy, WFBS’s Automatic Threat Response takes preemptive action by:

- Blocking shared folders to help prevent viruses/malware from infecting files in shared folders
• Blocking files with certain extensions on the Microsoft Exchange Server (Advanced only)

• Adding content filtering rules to the Messaging Security Agent (Advanced only)

• Blocking ports to help prevent viruses/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 viruses/malware from modifying files

• Assessing clients on your network for vulnerabilities that make them prone to the current outbreak

• Deploying the latest virus pattern file and Damage Cleanup Engine

• Performing a Cleanup on all the clients affected by the outbreak

• Scanning your clients and networks and taking action against detected threats (if enabled)

---

**Vulnerability Assessment**

Vulnerability Assessment provides system administrators or other network security personnel with the ability to assess security risks to their networks. The information they generate by using Vulnerability Assessment gives them a clear guide as to how to resolve known vulnerabilities and secure their networks.

Use Vulnerability Assessment to:

• Scan computers on your network for vulnerabilities.

• Identify vulnerabilities according to standard naming conventions. Find out more about the vulnerability and how to resolve it by clicking on the vulnerability name.
• Display the vulnerabilities by computer and IP address. Results include the risk level that the vulnerabilities represent to the computer and to the entire network.

• Report vulnerabilities according to individual computers and describe the security risks those computers present to the overall network.

• Configure tasks that scan any or all computers attached to a network. Scans can search for single vulnerabilities or a list of all known vulnerabilities.

• Run manual assessment tasks or set tasks to run according to a schedule.

• Request blocking for computers that present an unacceptable level of risk to network security.

• Create reports that identify vulnerabilities according to individual computers and describe the security risks those computers present to the overall network. The reports identify the vulnerability according to standard naming conventions so that Administrators can research further to resolve the vulnerabilities and secure the network.

• View assessment histories and compare reports to better understand the vulnerabilities and the changing risk factors to network security.

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 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 viruses/malware from modifying files

Outbreak Defense Current Status

Navigate to Outbreak Defense > Current Status to view and track the status of worldwide virus/malware outbreak threats.

During an outbreak, Worry-Free Business Security uses the Outbreak Defense strategy to protect your computers and networks. In each stage, it refreshes the information in the Current Status page.

Prevention

The Prevention stage of the Current Status screen displays information about recent threats, clients that have alerts enabled, and clients that are vulnerable to any reported threats.

• **Threat Information**: The Threat Information section displays information about viruses/malware that are currently on the Internet and could potentially affect your network and clients. Based on Threat Information, the Outbreak Prevention Policy takes steps to protect the network and clients while Trend Micro develops a solution (See Outbreak Prevention Policy on page 10-5). Learn more about a threat on the Trend Micro website select Help > Security Info.

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.
Using Outbreak Defense

• **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.

---

**Note**

The sections that follow are viewed only after an outbreak occurs.

---

**Vulnerable Computers**

The **Vulnerable Computers** section displays a list of clients that have vulnerabilities that make them susceptible to the threat displayed in the **Threat Information** section.

**Threat Protection**

The Threat Protection stage of the **Current Status** screen provides information about the Solution Download Status in regard to Trend Micro update components and the Solution Deployment Status in regard to all Agents.

• **Solution Download Status**: Displays a list of components that need to be updated in response to the threat listed in the Threat Information section.

• **Solution Deployment Status**: Displays the number of Agents that have updated and outdated components. It also provides links to view the clients with updated or outdated components.

**Threat Cleanup**

The Threat Cleanup stage of the **Current Status** screen displays the status of the scan that takes place after the updated components have been deployed. The Threat Cleanup stage also displays the status of clients after the scan and lists whether the updates were successful in cleaning or removing threat remnants.

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.

### Automatic Outbreak Defense Details

Navigate to **Outbreak Defense > Current Status > Prevention** to view automatic Outbreak Defense details.

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.

### Outbreak Defense Potential Threat

The Potential Threat screen (**Outbreak Defense > Potential Threat**) displays information about security risks to your clients and network. The Security Server gathers threat information by running Vulnerability Assessment and Cleanup Services to clean threats.
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 Computer(s)**

A vulnerable computer has weaknesses in its operating system or applications. Many threats exploit these vulnerabilities to cause damage or gain unauthorized control. Therefore, vulnerabilities represent risks not only to each individual computer where they are located, but also to the other computers on your network.

The Vulnerable Computers section lists all the clients on your network that have vulnerabilities discovered since the last vulnerability assessment. You can view the Last updated time in the top-right hand corner of the screen.

The Potential Threat screen ranks the clients according to the risk level that they pose to the network. Risk level is calculated by Trend Micro and represents the relative number and severity of vulnerabilities for each client.

When you click **Scan for Vulnerabilities Now**, Worry-Free Business Security 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.

**Computer(s) to Cleanup**

Cleanup runs in the background whenever Agents run Antivirus scans. You do not need to set up scheduled Cleanup scans. For details, see *Damage Cleanup Services on page 10-10.*
Vulnerability Assessment Pattern File

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

Damage Cleanup Services

Security Agents use Damage Cleanup Services to protect clients against Trojan horse programs (or Trojans). To address the threats and nuisances posed by Trojans and other malware, Damage Cleanup Services does the following:

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

To accomplish these tasks, Damage Cleanup Services makes use of these components:

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

Running Damage Cleanup Services

Damage Cleanup Services runs automatically. There is no need to configure it. Users are not aware when it is executed because it runs in the background (when Agents are running). However, the Security Server may sometimes notify the user to restart their computer to complete the cleanup.

Damage Cleanup Services runs on clients on these occasions:
• Administrators launch cleanup from the web console (Outbreak Defense > Potential Threat > Cleanup Now)

After clicking Cleanup Now, the Cleanup Notifying Progress screen appears temporarily to show you the progress of the notification and then is replaced with the Cleanup Notifying Results screen.

The Cleanup Notifying Results screen displays whether or not the Security Server has successfully notified an agent. Unsuccessful results occur when an agent is offline or in unexpected situations such as when there are network interruptions.

• Users run a Manual Scan
• Users perform a manual cleanup after a scan
• After hot fix or patch deployment
• When the Security Server starts

Configuring Outbreak Defense Settings

Before you begin

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.

The following settings are provided for optimal protection:

**Table 10-2. Recommended Outbreak Defense Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Automatic Outbreak Defense for Red Alerts issued by Trend Micro</td>
<td>Enabled</td>
</tr>
<tr>
<td>Disable Red Alerts after</td>
<td>2 days</td>
</tr>
<tr>
<td>Disable Red Alerts after required components deployed</td>
<td>Enabled</td>
</tr>
<tr>
<td>Setting</td>
<td>Recommended Value</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Automatic Desktop/Server scans</td>
<td>Enabled</td>
</tr>
<tr>
<td>Automatic Microsoft Exchange scans (Advanced only)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Enable Automatic Outbreak Defense for Yellow Alerts issued by Trend Mic</td>
<td>Disabled</td>
</tr>
<tr>
<td>Disable Yellow Alerts after</td>
<td>N/A</td>
</tr>
<tr>
<td>Disable Yellow Alerts after required pattern/engine deployed</td>
<td>N/A</td>
</tr>
<tr>
<td>Disable Yellow Alerts after required pattern/engine deployed.</td>
<td>N/A</td>
</tr>
<tr>
<td>Automatic Desktop/Server scans</td>
<td>Enabled</td>
</tr>
<tr>
<td>Automatic Microsoft Exchange scans (Advanced only)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Exceptions</td>
<td>Ports for the following services will not be blocked during Outbreak Defense Automatic Response:</td>
</tr>
<tr>
<td></td>
<td>• DNS</td>
</tr>
<tr>
<td></td>
<td>• NetBios</td>
</tr>
<tr>
<td></td>
<td>• HTTPS (secure web server)</td>
</tr>
<tr>
<td></td>
<td>• HTTP (web server)</td>
</tr>
<tr>
<td></td>
<td>• Telnet</td>
</tr>
<tr>
<td></td>
<td>• SMTP (Simple mail protocol)</td>
</tr>
<tr>
<td></td>
<td>• FTP (File transfer protocol)</td>
</tr>
<tr>
<td></td>
<td>• Internet Mail (POP3)</td>
</tr>
<tr>
<td>Scheduled Policy Download Settings</td>
<td>Frequency: Every 30 minutes</td>
</tr>
<tr>
<td></td>
<td>Source: Trend Micro ActiveUpdate Server</td>
</tr>
</tbody>
</table>
Procedure

1. Navigate to **Outbreak Defense > Settings > Outbreak Defense**.

2. Update the following options as required:

   - **Enable Outbreak Defense for Red Alerts issued by Trend Micro**: Outbreak Defense policies stay in effect until you click **Outbreak Defense > Current Status > Disable** or one of the disable settings are met. When the Security Server downloads a new Outbreak Prevention Policy, the old policy stops.

   - **Disable Red Alerts after x days**: The duration for the Outbreak Defense alert.

   - Perform automatic virus scan after required components deployed for:
     - **Desktops/Servers**
     - **Exchange servers** (Advanced only)

   - **Yellow Alert settings**: Configure the options for Yellow Alerts. See [*Yellow Alerts on page 10-2*](#).

   - **Exceptions**: The ports that will not be blocked during Outbreak Defense Automatic Response. See [*Outbreak Defense Exceptions on page 10-14*](#).

   **Note**

   When adding a new exception, ensure to select **Enable this exception**.

   - **Scheduled Policy Download Settings**: The settings for periodically downloading updated components.
     - **Frequency**
     - **Source**: The source of the updates.
       - **Trend Micro ActiveUpdate server** (default)
       - **Intranet location containing a copy of the current file**
       - **Other update source**: Any other update source on the web.
3. Click Save.

Outbreak Defense Exceptions

During Outbreak Defense, the Security Server might block ports to prevent threats from accessing the computers on your network. However, you might have ports that you always want to keep open to ensure communication between the Security Server and other computers and applications. You can add these ports to the exclusion list so that they will never be blocked even during Outbreak Defense.

WARNING!

Trend Micro designed Outbreak Defense to block ports most commonly used by attackers and malicious software. Adding exceptions to port blocking might leave your computers and networks vulnerable.

Procedure

2. Perform the following tasks.
<table>
<thead>
<tr>
<th><strong>Task</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
</table>
| Add an exception | a. Click the plus (+) icon for the **Exceptions** section.  
|               | b. Click **Add**.  
|               | A new screen opens.  
|               | c. Update the following options as required:  
|               | • **Enable this exception**  
|               | • **Description**  
|               | • **Protocol**  
|               | • Transmission Control Protocol (TCP)  
|               | • User Datagram Protocol (UDP)  
|               | • Internet Control Message Protocol (ICMP)  
|               | • **Ports**: Type a port range or individual ports for the exception. Separate multiple entries with semicolons (;).  
<p>|               | d. Click <strong>Add</strong>.                                                                 |</p>
<table>
<thead>
<tr>
<th>TASK</th>
<th>STEPS</th>
</tr>
</thead>
</table>
| Edit an exception | a. From the **Edit Exceptions** screen, select **Enable this exception**.  
   b. Type a description for your exception in the **Description** field.  
   c. From the **Protocol** drop-down list, select the communication method that you want to exclude. You can select:  
   • Transmission Control Protocol (TCP)  
   • User Datagram Protocol (UDP)  
   • Internet Control Message Protocol (ICMP)  
   d. Enter the ports to exclude.  
   • For a range of ports, select **Port range** and then enter the first number in the range and then the last.  
   • To exclude specific ports, select **Specified ports** and enter the specific port numbers.  
   e. Click **Save**. |
| Remove an exception | **Tip**  
   Disable an exception instead of removing it.  
   a. Click the plus (+) icon for the **Exceptions** section.  
   b. Select the exception and click **Remove**.  
   c. Click **OK** to confirm. |
| Remove ports from the exception list | a. Select a port to remove, and click the **Remove** icon.  
   b. Click **OK** on the confirmation prompt. |

3. Click **Save**.
Configuring Vulnerability Assessment Settings

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

Procedure

1. Navigate to Outbreak Defense > Settings.

2. From the Vulnerability Assessment tab, update the following options as required.

   • Enable Scheduled Vulnerability Prevention
     • Frequency: Select from Daily, Weekly, or Monthly. If you select Weekly or Monthly, set the day of the week or the day of the month.
     • Start time

   • Target
     • All groups: Scans all the clients that appear in the Group Management Tree on the Computers screen.
     • Specified group(s): Limit the vulnerability assessment scan to only the selected groups.

3. Click Save.
Chapter 11

Managing Global Settings

This chapter discusses global settings for agents and system settings for the Security Server.
Global Settings

From the web console, you can configure global settings for the Security Server and Security Agents.

**Proxy**

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

- Component updates and license notifications
- Web Reputation, Behavior Monitoring, and Smart Scan

For details, see *Configuring Internet Proxy Settings on page 11-3*.

**SMTP**

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

For details, see *Configuring SMTP Server Settings on page 11-4*.

**Desktop/Server**

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

For details, see *Configuring Desktop/Server Settings on page 11-5*.

**System**

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

For details, see *Configuring System Settings on page 11-11*. 
Configuring Internet Proxy Settings

If the Security Server and agents use a proxy server to connect to the Internet, specify proxy server settings in order to utilize the following features and Trend Micro services:

- **Security Server**: Component updates and license maintenance
- **Security Agents**: Web Reputation, URL Filtering, Behavior Monitoring, Smart Feedback, and Smart Scan
- **Messaging Security Agents** (Advanced only): Web Reputation and Anti-spam

**Procedure**

1. Navigate to **Preferences > Global Settings**.
2. From the **Proxy** tab, update the following as required:
   - Security Server Proxy

**Note**

Messaging Security Agents also use Security Server proxy settings.

- Use a proxy server for updates and license notifications
- Use SOCKS 4/5 proxy protocol
- Address: IPv4/IPv6 address or host name
- Port
- Proxy server authentication
  - User name
  - Password
- Security Agent Proxy
  - Use the credentials specified for the update proxy
Note

Security Agents use the Internet Explorer proxy server and port to connect to the Internet. Select this option only if Internet Explorer on clients and the Security Server share the same authentication credentials.

- User name
- Password

3. Click Save.

Configuring SMTP Server Settings

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

Procedure

1. Navigate to Preferences > Global Settings.

2. Click the SMTP tab and update the following as required:
   - **SMTP server**: The IPv4 address or name of the SMTP server.
   - **Port**
   - **Enable SMTP Server Authentication**
     - **User Name**
     - **Password**

3. To verify that the settings are correct, click **Send Test Email**. If sending was unsuccessful, modify the settings or check the status of the SMTP server.

4. Click **Save**.
Configuring Desktop/Server Settings

The Desktop/Server options pertain to the Worry-Free Business Security global settings. Settings for individual groups override these settings. If you have not configured a particular option for a group, the Desktop/Server Options are used. For example, if no URLs are approved for a particular group, all the URLs approved on this screen will be applicable for the group.

Procedure

1. Navigate to Preferences > Global Settings.
2. Click the Desktop/Server tab and update the following as required:
<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Location Awareness       | With Location Awareness, administrators can control security settings depending on how the client is connected to the network. Location Awareness controls the In Office/Out of Office connection settings. The Security Agent automatically identifies the location of the client based on the gateway information configured on the web console, and then controls the websites users can access. The restrictions differ based on the user's location:  
  - **Enable location awareness**: These settings will affect the In Office/Out of Office connection settings of Firewall, Web Reputation, and frequency of scheduled updates.  
  - **Gateway Information**: Clients and connections in this list will use Internal Connection settings while remotely connecting to the network (using VPN) and Location Awareness is enabled.  
    - Gateway IP address  
    - MAC address: Adding the MAC address greatly improves security by permitting only the configured device to connect.  
  Click the corresponding trash can icon to delete an entry. |
| Help Desk Notice         | The Help Desk Notice places a notification on the Security Agent informing the user who to contact for help. Update the following as required:  
  - **Label**  
  - **Help Desk Email Address**  
  - **Additional Information**: This will pop-up when the user mouses over the label |
<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Scan Settings</td>
<td><strong>Disable Smart Scan Service</strong>: Switches all Security Agents to Conventional Scan mode. Smart Scan will not be available until it is enabled again here. To switch one or several Security Agent groups, navigate to Security Settings &gt; {Group} &gt; Configure &gt; Scan Method.</td>
</tr>
<tr>
<td></td>
<td><strong>Exclude the Security Server database folder</strong>: Prevents Agents installed on the Security Server from scanning its own database only during Real-time Scans. By default, WFBS does not scan its own database. Trend Micro recommends preserving this selection to prevent any possible corruption of the database that may occur during scanning.</td>
</tr>
<tr>
<td></td>
<td><strong>Exclude Microsoft Exchange server folders when installed on Microsoft Exchange server</strong>: Prevents Agents installed on the Microsoft Exchange server from scanning Microsoft Exchange folders.</td>
</tr>
<tr>
<td></td>
<td><strong>Exclude Microsoft Domain Controller folders</strong>: Prevents Agents installed on the Domain Controller from scanning Domain Controller folders. These folders store user information, user names, passwords, and other important information.</td>
</tr>
</tbody>
</table>
|                               | **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

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

## Spyware/Grayware Scan Settings

- **Add cookie into spyware log**: Adds each detected spyware cookie to the spyware log.

## Firewall Settings

- **Disable Firewall and uninstall drivers**: Check box to uninstall the WFBS client firewall and remove the drivers associated with the firewall.

**Note**

If you disable the firewall, related settings will not be available again until you re-enable the firewall.
### Web Reputation and URL Filtering

- **Process Exception List**: Processes excluded from Web Reputation and URL Filtering verifications. Type critical processes that your organization deems trustworthy.

  **Tip**
  When you update the process exception list and the server deploys the updated list to agents, all active HTTP connections on the client computer (through port 80, 81, or 8080) will be disconnected for a few seconds. Consider updating the process exception list during off-peak hours.

- **Send Web Reputation and URL Filtering logs to the Security Server**

### IM Content Filtering

Administrators can restrict the usage of certain words or phrases in instant messaging applications. Any message containing restricted words or phrases will not be delivered and the administrator will be notified.

Agents can restrict words used in the following IM applications: ICQ®, MSN™ Messenger, Windows Messenger Live™, Yahoo!™ Messenger

- **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

**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.
### SETTINGs

<table>
<thead>
<tr>
<th><strong>Watchdog Settings</strong></th>
<th>The Watchdog option ensures that the Security Agent is constantly protecting clients. When enabled, the Watchdog checks the availability of the Agent every ( x ) minutes. If the Agent is unavailable, the Watchdog will attempt to restart the Agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable the Security Agent Watchdog service</strong>: Trend Micro recommends enabling the Watchdog service to help ensure that the Security Agent is protecting your clients. If the Security Agent unexpectedly terminates, which could happen if the client is under attack from a hacker, the Watchdog service restarts the Security Agent.</td>
<td></td>
</tr>
<tr>
<td><strong>Check client status every ( {} ) minutes</strong>: Determines how often the Watchdog service should check client status.</td>
<td></td>
</tr>
<tr>
<td><strong>If the client cannot be started, retry ( {} ) times</strong>: Determines how many times the Watchdog service should attempt to restart the Security Agent.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Security Agent Uninstallation Password</strong></th>
<th><strong>Allow the client user to uninstall Security Agent without a password.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Require a password for the client user to uninstall Security Agent.</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Security Agent Program Exit and Unlock Password</strong></th>
<th><strong>Allow the client users to exit and unlock the Security Agent on their computer without a password.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Require client users to enter a password to exit and unlock the Security Agent.</strong></td>
<td></td>
</tr>
</tbody>
</table>

#### Note

Unlocking the Security Agent allows the user to override all settings configured under **Security Settings \( \{\text{group}\} \) > Configure > Client Privileges.**
### Managing Global Settings

<table>
<thead>
<tr>
<th><strong>SETTINGS</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Preferred IP Address</td>
<td>This setting is only available on dual-stack Security Servers and is applied only by dual-stack agents. After you install or upgrade agents, the agents register to the Security Server using an IP address. Choose from the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>IPv4 first, then IPv6</strong>: Agents use their IPv4 address first. If the agent cannot register using its IPv4 address, it uses its IPv6 address. If registration is unsuccessful using both IP addresses, the agent retries using the IP address priority for this selection.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IPv6 first, then IPv4</strong>: Agents use their IPv6 address first. If the agent cannot register using its IPv6 address, it uses its IPv4 address. If registration is unsuccessful using both IP addresses, the agent retries using the IP address priority for this selection.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

## Configuring System Settings

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.

### Procedure

1. Navigate to **Preferences > Global Settings**.
2. Click the **System** tab and update the following as required:
Inactive Security Agent Removal

When you use the Security Agent uninstallation program on the client to remove the Agents from a client, the program automatically notifies the Security Server. When the Security Server receives this notification, it removes the client icon from the Security Groups Tree to show that the client no longer exists.

However, if the Security Agent is removed using other methods, such as reformatting the computer’s hard drive or deleting the client files manually, the Security Server will be unaware of the removal and will display the Security Agent as inactive. If a user unloads or disables the Agent for an extended time, the Security Server also displays the Security Agent as inactive.

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

- **Enable automatic removal of inactive Security Agent:** Enables the automatic removal of clients that have not contacted the Security Server for the specified number of days.

- **Automatically remove a Security Agent if inactive for {} days:** The number of days that a client is allowed to be inactive before it is removed from the web console.
### Settings | Description
--- | ---
Agent Connection Verification | WFBS represents the client connection status in the Security Groups Tree using icons. However, certain conditions may prevent the Security Groups Tree from displaying the correct agent connection status. For example, if the network cable of a client is accidentally unplugged, the agent will not be able to notify the Trend Micro Security Server that it is now offline. This agent will still appear as online in the Security Groups Tree.

You can verify agent-server connection manually or schedule the verification from the web console.

**Note**
Connection Verification does not allow the selection of specific groups or agents. It verifies the connection of all agents registered with the Security Server.

- **Enable scheduled verification**: Enables scheduled verification of agent-server connection.
  - Hourly
  - Daily
  - Weekly, every
  - **Start time**: The time the verification should start.
- **Verify Now**: Instantly tests the connectivity.
### Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine</td>
<td>By default, Security Agents send quarantined infected files to the following directory in the Security Server:</td>
</tr>
<tr>
<td>Maintenance</td>
<td><code>&lt;Security Server installation folder&gt;\PCCSRV\Virus</code></td>
</tr>
<tr>
<td></td>
<td>If you need to change the directory (for example, if it has insufficient disk space), type an absolute path, such as <code>D: \Quarantined Files</code>, in the Quarantine Directory field. If you do this, be sure to also apply the same changes in Security Settings &gt; {Group} &gt; Configure &gt; Quarantine or agents will continue sending the files to <code>&lt;Security Server installation folder&gt;\PCCSRV\Virus</code>.</td>
</tr>
<tr>
<td></td>
<td>In addition, configure the following maintenance settings:</td>
</tr>
<tr>
<td></td>
<td>• Quarantine folder capacity: The size of the quarantine folder in MB.</td>
</tr>
<tr>
<td></td>
<td>• Maximum size for a single file: The maximum size of a single file stored in the quarantine folder in MB.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>If you do not want agents to send quarantined files to the Security Server, configure the new directory in Security Settings &gt; Configure &gt; Quarantine and ignore all the maintenance settings. See Quarantine Directory on page 5-28 for instructions.</td>
</tr>
<tr>
<td>Security Agent</td>
<td><strong>Security Agent Installation directory</strong>: During installation, you are prompted to type the Security Agent installation directory, which is where Setup installs each Security Agent.</td>
</tr>
<tr>
<td>Installation</td>
<td>If needed, change the directory by typing an absolute path. Only future agents will be installed to this directory; existing agents maintain their current directory.</td>
</tr>
<tr>
<td></td>
<td>Use one of the following variables to set the installation path:</td>
</tr>
<tr>
<td></td>
<td>• <code>$BOOTDISK</code>: The drive letter of the boot disk</td>
</tr>
<tr>
<td></td>
<td>• <code>$WINDIR</code>: The folder where Windows is installed</td>
</tr>
<tr>
<td></td>
<td>• <code>$ProgramFiles</code>: The programs folder</td>
</tr>
</tbody>
</table>
3. Click **Save**.
Using Logs and Reports

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

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

**Note**

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

WFBS maintains logs under the following categories:

- Web Console event logs
- Desktop/Server logs
- Microsoft Exchange server logs (Advanced only)

**Table 12-1. Log Type and Content**

<table>
<thead>
<tr>
<th>TYPE (ENTITY THAT GENERATED THE LOG ENTRY)</th>
<th>CONTENT (TYPE OF LOG TO OBTAIN CONTENT FROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management console events</td>
<td>• Manual Scan (launched from the web console)</td>
</tr>
<tr>
<td></td>
<td>• Update (Security Server updates)</td>
</tr>
<tr>
<td></td>
<td>• Outbreak Defense events</td>
</tr>
<tr>
<td></td>
<td>• Console events</td>
</tr>
<tr>
<td><strong>TYPE (ENTITY THAT GENERATED THE LOG ENTRY)</strong></td>
<td><strong>CONTENT (TYPE OF LOG TO OBTAIN CONTENT FROM)</strong></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Desktop/Server</td>
<td>• Virus logs</td>
</tr>
<tr>
<td></td>
<td>• Manual Scan</td>
</tr>
<tr>
<td></td>
<td>• Real-time Scan</td>
</tr>
<tr>
<td></td>
<td>• Scheduled scan</td>
</tr>
<tr>
<td></td>
<td>• Cleanup</td>
</tr>
<tr>
<td></td>
<td>• Spyware/Grayware logs</td>
</tr>
<tr>
<td></td>
<td>• Manual Scan</td>
</tr>
<tr>
<td></td>
<td>• Real-time Scan</td>
</tr>
<tr>
<td></td>
<td>• Scheduled scan</td>
</tr>
<tr>
<td></td>
<td>• Web Reputation logs</td>
</tr>
<tr>
<td></td>
<td>• URL Filtering logs</td>
</tr>
<tr>
<td></td>
<td>• Behavior monitoring logs</td>
</tr>
<tr>
<td></td>
<td>• Update logs</td>
</tr>
<tr>
<td></td>
<td>• Network virus logs</td>
</tr>
<tr>
<td></td>
<td>• Outbreak Defense logs</td>
</tr>
<tr>
<td></td>
<td>• Event logs</td>
</tr>
<tr>
<td></td>
<td>• Device Control logs</td>
</tr>
<tr>
<td></td>
<td>• Hot Fix Deployment logs</td>
</tr>
</tbody>
</table>
Using Log Query

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

A Messaging Security Agent (Advanced only) sends its logs to the Security Server every five minutes (regardless of when the log is generated).

**Procedure**

1. Navigate to Reports > Log Query.
2. Update the following options as required:
   - **Time Range**
     - Preconfigured range
     - Specified range: To limit the query to certain dates.
   - **Type**: See Logs on page 12-2 to view the contents of each log type.

---

<table>
<thead>
<tr>
<th>TYPE (ENTITY THAT GENERATED THE LOG ENTRY)</th>
<th>CONTENT (TYPE OF LOG TO OBTAIN CONTENT FROM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange server (Advanced only)</td>
<td>• Virus logs</td>
</tr>
<tr>
<td></td>
<td>• Attachment Blocking logs</td>
</tr>
<tr>
<td></td>
<td>• Content Filtering/Data Loss Prevention logs</td>
</tr>
<tr>
<td></td>
<td>• Update logs</td>
</tr>
<tr>
<td></td>
<td>• Backup logs</td>
</tr>
<tr>
<td></td>
<td>• Archive logs</td>
</tr>
<tr>
<td></td>
<td>• Outbreak Defense logs</td>
</tr>
<tr>
<td></td>
<td>• Scan Event logs</td>
</tr>
<tr>
<td></td>
<td>• Unscannable Message Parts logs</td>
</tr>
<tr>
<td></td>
<td>• Web Reputation logs</td>
</tr>
</tbody>
</table>
- Management console events
- Desktop/Server
- Exchange server (Advanced only)

- Content: The available options depend on the Type of log.

3. Click Display Logs.

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

---

**Reports**

You can manually generate one-time reports or set the Security Server to generate scheduled reports.

You can print reports or send them by email to an administrator or to other individuals.

The data available in a report is influenced by the amount of logs available on the Security Server at the time the report was generated. The amount of logs changes as new logs are added and existing ones deleted. In Reports > Maintenance, you can manually delete logs or set a log deletion schedule.

**Working with One-time Reports**

**Procedure**

1. Navigate to Reports > One-time Reports.

2. Perform the following tasks:
<table>
<thead>
<tr>
<th><strong>Task</strong></th>
<th><strong>Steps</strong></th>
</tr>
</thead>
</table>
| Generate a report | a. Click **Add**.  
A new screen appears.  
b. Configure the following:  
* **Report name**  
* **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 the plus icon (+) to expand the selection.  
* **Send the report to**  
  * **Recipients**: Type the recipients’ email addresses, separating them with semicolons (;).  
  * **Format**: Choose PDF or a link to an HTML report. If you choose PDF, the PDF will be attached to the email.  
c. Click **Add**. |
| View the report | Under the Report Name column, click the links to the report. The first link opens a PDF report while the second link opens an HTML report.  
The data available in a report is influenced by the amount of logs available on the Security Server at the time the report was generated. The amount of logs changes as new logs are added and existing ones deleted. In **Reports > Maintenance**, you can manually delete logs or set a log deletion schedule.  
For details on the content of the report, see *Interpreting Reports on page 12-11*. |
## Using Logs and Reports

### Delete reports

<table>
<thead>
<tr>
<th>TASK</th>
<th>STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>a. Select the row containing the report links.</td>
</tr>
<tr>
<td></td>
<td>b. Click Delete.</td>
</tr>
</tbody>
</table>

**Note**

To automatically delete reports, navigate to Reports > Maintenance > Reports tab and set the maximum number of one-time reports that WFBS retains. The default is 10 one-time reports. When the number is exceeded, the Security Server deletes reports beginning with the report that has been retained for the longest time.

---

### Working with Scheduled Reports

**Procedure**

1. Navigate to Reports > Scheduled Reports.
2. Perform the following tasks:
### Task: Create a scheduled report template

<table>
<thead>
<tr>
<th>Steps</th>
</tr>
</thead>
</table>
| a. Click **Add**.  
A new screen appears.  

b. Configure the following:  

- **Report template name**  
- **Schedule**: Daily, weekly, or monthly, and the time to generate the report  
  For monthly reports, if you select 31, 30, or 29 days and a month has less than the number of days, WFBS will not generate the report that month.  
- **Content**: To select all threats, select the **Select All** check box. To select individual threats, click the corresponding check box. Click the plus icon (+) to expand the selection.  
- **Send the report to**  
  - **Recipients**: Type the recipients’ email addresses, separating them with semicolons (;).  
  - **Format**: Choose PDF or a link to an HTML report. If you choose PDF, the PDF will be attached to the email. |
| c. Click **Add**. |
### View scheduled reports

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>View scheduled reports</td>
<td>a. On the row containing the template from which the scheduled reports are generated, click <strong>Report History</strong>. A new screen opens.</td>
</tr>
<tr>
<td></td>
<td>b. Under the View column, click the links to a report. The first link opens a PDF report while the second link opens an HTML report.</td>
</tr>
<tr>
<td></td>
<td>The data available in a report is influenced by the amount of logs available on the Security Server at the time the report was generated. The amount of logs changes as new logs are added and existing ones deleted. In <strong>Reports &gt; Maintenance</strong>, you can manually delete logs or set a log deletion schedule.</td>
</tr>
<tr>
<td></td>
<td>For details on the content of the report, see <em>Interpreting Reports on page 12-11</em>.</td>
</tr>
</tbody>
</table>

### Template Maintenance Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit template settings</td>
<td>Click the template and then edit the settings in the new screen that appears. Reports generated after saving your changes will use the new settings.</td>
</tr>
<tr>
<td>Enable/Disable a template</td>
<td>Click the icon under the Enabled column. Disable a template if you want to stop generating scheduled reports temporarily and enable it when you need the reports again.</td>
</tr>
</tbody>
</table>
Delete a template

Select the template and click **Delete**.

Deleting a template does not delete scheduled reports generated from the template but the links to the reports will no longer be available from the web console. You can access the reports directly from the Security Server computer. Reports will only be deleted if you manually delete them from the computer or if the Security Server automatically deletes the reports according to the scheduled report auto-deletion setting in **Reports > Maintenance > Reports** tab.

To automatically delete templates, navigate to **Reports > Maintenance > Reports** tab and set the maximum number of templates that WFBS retains. The default is 10 templates. When the number is exceeded, the Security Server deletes templates beginning with the template that has been retained for the longest time.

---

**Report Maintenance Tasks**

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send a link to the scheduled reports</td>
<td>Send a link to the scheduled reports (in PDF format) through email. Recipients click the link in the email message to access the PDF file. Be sure that recipients can connect to the Security Server computer or the file will not display.</td>
</tr>
</tbody>
</table>

**Note**

Only a link to the PDF file is provided in the email. The actual PDF file is not attached.

a. On the row containing the template from which the scheduled reports are generated, click **Report History**.
   A new screen opens.

b. Select the reports and then click **Send**.
   Your default email client opens, with a new email containing a link to the report.
Delete scheduled reports

<table>
<thead>
<tr>
<th>TASK</th>
<th>STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete scheduled</td>
<td>a. On the row containing the template from which the scheduled reports are generated, click <strong>Report History</strong>. A new screen opens.</td>
</tr>
<tr>
<td>reports</td>
<td>b. Select the reports and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

**Note**

To automatically delete reports, navigate to **Reports > Maintenance > Reports** tab and set the maximum number of scheduled reports in each template that WFBS retains. The default is 10 scheduled reports. When the number is exceeded, the Security Server deletes reports beginning with the report that has been retained for the longest time.

---

**Interpreting Reports**

Worry-Free Business Security reports contain the following information. The information displayed could vary depending on the options selected.
### Table 12-2. Contents of a Report

<table>
<thead>
<tr>
<th>Report Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td><strong>Desktop/Servers Virus Summary</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td>Top 5 Desktop/Servers with Virus Detections</td>
<td>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</td>
</tr>
<tr>
<td>Outbreak Defense History</td>
<td><strong>Outbreak Defense History</strong>&lt;br&gt;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).</td>
</tr>
<tr>
<td>Anti-spyware</td>
<td><strong>Desktop/Servers Spyware/Grayware Summary</strong>&lt;br&gt;The spyware/grayware report shows detailed information about the spyware/grayware threats detected on clients, including the number of detections and the actions that WFBS took against them. The report includes a pie chart that shows the percentage of each anti-spyware scan action that has been performed.</td>
</tr>
<tr>
<td>Top 5 Desktop/Servers with Spyware/Grayware Detections</td>
<td>The report also shows the top five spyware/grayware threats detected and the five desktops/servers with the highest number of spyware/grayware detected. To learn more about the spyware/grayware threats that have been detected, click the spyware/grayware names. A new web browser page opens and displays related information on the spyware/grayware on the Trend Micro website.</td>
</tr>
<tr>
<td>REPORT ITEM</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Anti-spam summary</strong> (Advanced only)</td>
<td><strong>Spam Summary</strong>&lt;br&gt;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.</td>
</tr>
<tr>
<td>Web Reputation</td>
<td><strong>Top 10 Computers Violating Web Reputation Policies</strong></td>
</tr>
</tbody>
</table>
| URL category | **Top 5 URL Category Policies Violated**<br>Lists the most commonly accessed website categories that violated the policy.  
**Top 10 Computers Violating URL Category Policies** |
| Behavior Monitoring | **Top 5 Programs Violating Behavior Monitoring Policies**  
**Top 10 Computers Violating Behavior Monitoring Policies** |
| Device Control | **Top 10 Computer Violating Device Control Policy** |
| **Content filtering summary** (Advanced only) | **Content Filtering Summary**<br>Content filtering reports show information about the total number of messages that the Messaging Security Agent filtered.  
**Top 10 Content Filtering Rules Violated**<br>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**<br>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**<br>List the computers on your network that report the most frequent virus incidents. |
Performing Maintenance Tasks for Reports and Logs

Procedure

1. Navigate to Reports > Maintenance.

2. Perform the following tasks:

<table>
<thead>
<tr>
<th>TASK</th>
<th>STEPS</th>
</tr>
</thead>
</table>
| Set the maximum number of reports and templates | You can limit the number of one-time reports, scheduled reports (per template), and templates available on the Security Server. When the number is exceeded, the Security Server deletes reports/templates beginning with the report/template that has been retained for the longest time.  
  a. Click the Reports tab.  
  b. Type the maximum number of one-time reports, scheduled reports, and report templates to retain. |
| Configure automatic deletion of logs           | a. Click the Auto Log Deletion tab.  
  b. Select log types and specify the maximum age of the logs. Logs older than this value will be deleted. |
| Manually delete logs                           | a. Click the Manual Log Deletion tab.  
  b. For each log type, type the maximum age of the logs. Logs older than this value will be deleted. To delete all the logs, type 0.  
  c. Click Delete. |

3. Click Save.
Chapter 13

Performing Administrative Tasks

This chapter explains how to perform additional administrative tasks such as viewing the product license, working with Plug-in Manager, and uninstalling the Security Server.
Changing the Web Console Password

Trend Micro recommends using strong passwords for the web console. A strong password is at least eight characters long, has one or more uppercase letters (A-Z), has one or more lowercase letters (a-z), has one or more numerals (0-9), and has one or more special characters or punctuation marks (!@#$%^&,.:;?). Strong passwords never are the same as the user’s login name or contain the login name in the password itself. They do not consist of the user’s given or family name, birth dates, or any other item that is easily identified with the user.

Procedure

1. Navigate to Preferences > Password.

2. Update the following options as required:
   - Old password
   - New password
   - Confirm password: Re-type the new password to confirm.

3. Click Save.

Working with Plug-in Manager

Plug-in Manager displays the programs for both the Security Server 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 from Preferences > Plug-Ins. After the installation, you can check for available plug-in programs. See the documentation for Plug-in Manager and plug-in programs for more information.
Managing the Product License

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

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 have very limited protection. Use the Product License screen to determine your license expiration date to ensure that you renew your license before it expires.

Note

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.

License Renewal

You can renew or upgrade to a fully licensed version of WFBS by purchasing a maintenance renewal. The fully licensed version requires an Activation Code.

Renew the product license in two ways:

• On the web console, navigate to the Live Status screen and follow the on-screen instructions. These instructions appear 60 days before and 30 days after the license expires.

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

Resellers can leave their contact information on a file on the Security Server. Check the file at:

{Security Server installation folder}\PCCSRV\Private\contact_info.ini
Note

{Security Server installation folder} is typically C:\Program Files \Trend Micro\Security Server.

A Trend Micro representative will update your registration information using Trend Micro Product Registration.

The Security Server polls the Product Registration server and receives the new expiration date directly from the Product Registration server. You do not need to manually enter a new Activation Code when renewing your license.

Activating a New License

Your license type determines your Worry-Free Business Security Activation Code.

**TABLE 13-1. Activation Code by License Type**

<table>
<thead>
<tr>
<th>LICENSE TYPE</th>
<th>ACTIVATION CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully licensed version of WFBS Standard</td>
<td>CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx</td>
</tr>
<tr>
<td>Fully licensed version of WFBS Advanced</td>
<td>CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx</td>
</tr>
</tbody>
</table>

**Note**

If you have questions about the Activation Code, please consult the Trend Micro support website at:

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

Use the Product License screen to change your license type by entering a new Activation Code.

1. Navigate to **Preferences > Product License**.
2. Click **Enter a new code**.
3. Type your new Activation Code in the space provided.
4. Click **Activate**.

## Participating in the Smart Feedback Program

For details about Smart Feedback, see *Smart Feedback on page 1-5*.

### Procedure

1. Navigate to **Preferences > Smart Protection Network**.
2. Click **Enable Trend Micro Smart Feedback**.
3. To send information about potential security threats in the files on your client computers, select the **Enable feedback of suspicious program files** check box.

### Note

Files sent to Smart Feedback contain no user data and are submitted only for threat analysis.

4. To help Trend Micro understand your organization, select the **Industry** type.
5. Click **Save**.

## Changing the Agent’s Interface Language

By default, the language used on the agent interface will correspond to the locale configured on the client operating system. Users can change the language from the agent interface.
Saving and Restoring Program Settings

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

Procedure


2. Manually copy the following files and folders from the folder to an alternate location:

   - ofcscan.ini: Contains global settings.
   - ous.ini: Contains the update source table for antivirus component deployment.

   **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.
Performing Administrative Tasks

- **Private folder**: Contains firewall and update source settings.
- **Web\TmOPP folder**: Contains Outbreak Defense settings.
- **Pccnt\Common\OfcPfw.dat**: Contains firewall settings.
- **Download\OfcPfw.dat**: Contains firewall deployment settings.
- **Log folder**: Contains system events and the verify connection log.
- **Virus folder**: The folder in which WFBS quarantines infected files.
- **HTTDB folder**: Contains the WFBS database.


4. Perform a fresh install. See the WFBS *Installation and Upgrade Guide*.

5. After the master installer finishes, stop the Trend Micro Security Server Master Service on the target computer.

6. Update the virus pattern version from the backup file:
   a. Get current virus pattern version from the new server.
      
      \Trend Micro\Security Server\PCCSRV\Private\component.ini. [6101]
      
      ComponentName=Virus pattern
      
      Version=xxxxxxx 0 0
   
   b. Update the version of the virus pattern in the backed-up file:
      
      \Private\component.ini

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

7. With the backups you created, overwrite the WFBS database and the relevant files and folders on the target machine in the PCCSRV folder.

Uninstalling the Security Server

Uninstalling the Security Server also uninstalls the Scan Server.

Worry-Free Business Security 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.


Procedure

1. On the computer you used to install the server, click Start > Control Panel > Add or Remove Programs.

2. Click Trend Micro Security Server, and then click Change/Remove.

   A confirmation screen appears.

3. Click Next.

   Master Uninstaller, the server uninstallation program, prompts you for the Administrator password.

4. Type the Administrator password in the text box and click OK.

   Master Uninstaller then starts removing the server files. A confirmation message appears after Security Server has been uninstalled.

5. Click OK to close the uninstallation program.
Chapter 14

Using Management Tools

This chapter explains how to use the administrative and client tools and add-ins.
Tool Types

Worry-Free Business Security includes a set of tools that can help you easily accomplish various tasks, including server configuration and client management.

**Note**

Administrative and client tools cannot be launched from the web console. Add-ins can be downloaded 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**
  - **Login Script Setup** (*SetupUsr.exe*): Automates the Security Agent installation. See *Installing with Login Script Setup on page 3-13*.
  - **Vulnerability Scanner** (*TMVS.exe*): Locates unprotected computers on the network. See *Installing with Vulnerability Scanner on page 3-21*.
  - **Remote Manager Agent**: Enables Resellers to manage WFBS through a centralized web console. See *Installing the Trend Micro Worry-Free Remote Manager Agent on page 14-3*.
  - **Trend Micro Disk Cleaner**: Deletes unnecessary WFBS backup files, log files and unused pattern files. See *Saving Disk Space on page 14-5*.
  - **Scan Server Database Mover**: Moves the Scan Server database safely to another disk drive. See *Moving the Scan Server Database on page 14-8*.

- **Client tools**
  - **Client Packager** (*ClnPack.exe*): Creates a self-extracting file containing the Security Agent and components. See *Installing with Client Packager on page 3-14*.
  - **Restore Encrypted Virus** (*VSEncode.exe*): Opens infected files encrypted by WFBS. See *Restoring Encrypted Files on page 14-9*. 

Using Management Tools

- **Client Mover Tool** (*IpXfer.exe*): Transfers agents from one Security Server to another. See *Moving Agents on page 4-12*.

- **Regenerate the Security Agent ClientID** (*regenid.exe*): Use the ReGenID utility to regenerate the Security Agent ClientID, based on whether the Agent is on a cloned computer or a virtual machine. See *Using the ReGenID Tool on page 14-13*.

- **Security Agent Uninstall** (*SA_Uninstall.exe*): automatically removes all Security Agent components from client machine. See *Using the SA Uninstall Tool on page 3-40*.

- **Add-ins**: Allow administrators to view live security and system information from the consoles of supported Windows operating systems. This is the same high-level information visible on the Live Status screen. See *Managing SBS and EBS Add-ins on page 14-14*.

---

**Note**

Some tools available in previous versions of WFBS are not available in this version. If you require these tools, contact Trend Micro Technical Support.

---

**Installing the Trend Micro Worry-Free Remote Manager Agent**

The Worry-Free Remote Manager Agent allows resellers to manage WFBS with Worry-Free Remote Manager (WFRM). The WFRM Agent (version 3.0) is installed on Security Server 8.0.

If you are a Trend Micro certified partner, you can install the agent for Trend Micro Worry-Free Remote Manager (WFRM). If you chose not to install the WFRM agent after the Security Server installation completes, you can do so later.

Installation requirements:

- WFRM Agent GUID
To obtain the GUID, open the WFRM Console and go to Customers (tab) > All Customers (on the tree) > {customer} > WFBS/CSM > Server/Agent Details (right pane) > WFRM Agent Details

- An active Internet connection
- 50MB of free disk space

Procedure

1. Go to the Security Server and navigate to the following installation folder: \PCCSRV\Admin\Utility\RmAgent, and launch the application WFRMAgentforWFBS.exe.

   For example: C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility\RmAgent\WFRMAgentforWFBS.exe

   **Note**
   
   Skip this step if you are launching the installation from the Security Server Setup screen.

2. In the Worry-Free Remote Manager Agent Setup Wizard, read the license agreement. If you agree with the terms, select I accept the terms of the license agreement and then click Next.

3. Click Yes to confirm that you are a certified partner.

4. Select I already have a Worry-Free Remote Manager account and I want to install the agent. Click Next.

5. Determine your scenario.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>New customer</td>
<td>a. Select <strong>Associate with a new customer.</strong></td>
</tr>
<tr>
<td></td>
<td>b. Click <strong>Next.</strong> Enter the customer information.</td>
</tr>
</tbody>
</table>
### Using Management Tools

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note</strong>&lt;br&gt;If the customer already exists on the WFRM Console and you use the option above to associate with a new customer, this will result in two duplicate customers with the same name appearing on the WFRM network tree. To avoid this, use the method below.</td>
</tr>
</tbody>
</table>
| Existing customer | a. Select **This product already exists in Remote Manager.**<br>**Note**<br>WFBS must already have been added to the WFRM Console. See your WFRM documentation for instructions.  
|                | b. Type the GUID.  |

6. Click **Next**.

7. Select the **Region** and **Protocol**, and enter the Proxy information if required.

8. Click **Next**.

   The Installation Location screen opens.

9. To use the default location, click **Next**.

10. Click **Finish**.

    If the installation is successful and settings are correct, the WFRM Agent should automatically register to the Worry-Free Remote Manager server. The Agent should show as Online on the WFRM Console.

---

### Saving Disk Space

Save disk space on the Security Server and clients by running Disk Cleaner.
Running Disk Cleaner on the Security Server

Before you begin

To save disk space, the Disk Cleaner Tool (TMDiskCleaner.exe) identifies and deletes unused backup, log, and pattern files from the following directories:

- {Security Agent}\AU_Data\AU_Temp\*
- {Security Agent}\Reserve
- {Security Server}\PCCSRV\TEMP\* (except hidden files)
- {Security Server}\PCCSRV\Web\Service\AU_Data\AU_Temp\*
- {Security Server}\PCCSRV\wss\*.log
- {Security Server}\PCCSRV\wss\AU_Data\AU_Temp\*
- {Security Server}\PCCSRV\Backup\*
- {Security Server}\PCCSRV\Virus\* (Deletes quarantined files older than two weeks, except the NOTVIRUS file)
- {Security Server}\PCCSRV\ssaptpn.xxx (keeps the latest pattern only)
- {Security Server}\PCCSRV\lpt$vpn.xxx (keeps the latest three patterns only)
- {Security Server}\PCCSRV\icrc$oth.xxx (keeps the latest three patterns only)
- {Security Server}\DBBackup\* (keeps latest two subfolders only)
- {Messaging Security Agent}\AU_Data\AU_Temp\*
- {Messaging Security Agent}\Debug\*
- {Messaging Security Agent}\engine\vsapi\latest\pattern\*
Using Management Tools

Procedure
1. On the Security Server, go to the following directory:
   {Server Installation Folder}\PCCSRV\Admin\Utility\n2. Double-click TMDiskCleaner.exe.

   Note
   Files cannot be restored.

3. Click Delete Files to scan for and delete unused backup, log, and pattern files.

Running Disk Cleaner on the Security Server Using the Command Line Interface

Procedure
2. At the command prompt, run the following command:

   TMDiskCleaner.exe [/hide] [/log] [/allowundo]

   • /hide: Runs the tool as a background process.
   • /log: Saves a log of the operation to DiskClean.log that resides in the current folder.

   Note
   /log is available only when /hide is used.

   • /allowundo: Moves the files to the Recycle Bin and does not permanently delete the files.
3. To run the Disk Cleaner tool frequently, configure a new task using Windows Scheduled Tasks. See the Windows documentation for more information.

Saving Disk Space on Clients

Procedure

• On desktops/servers with Security Agents:
  • Clean up quarantine files
  • Clean up log files
  • Run the Windows Disk Cleanup Utility

• On Microsoft Exchange Servers with Messaging Security Agents:
  • Clean up quarantine files
  • Clean up log files
  • Run the Windows Disk Cleanup Utility
  • Clean up archive logs
  • Clean up backup files
  • Check the size of the Microsoft Exchange database or transaction logs

Moving the Scan Server Database

If the disk drive on which the Scan Server is installed has insufficient disk space, use the Scan Server Database Mover tool to safely move the Scan Server database to another disk drive.

Be sure that the Security Server computer has more than 1 disk drive and that the new disk drive has at least 3GB of available disk space. Mapped drives are not accepted. Do not move the database manually or use other tools.
Procedure

1. On the Security Server computer, navigate to `<Security Server installation folder>`\PCCSRV\Admin\Utility.
2. Launch ScanServerDBMover.exe.
3. Click Change.
4. Click Browse and then browse to the target directory on the other disk drive.
5. Click OK and then Complete when the database has been moved.

Restoring Encrypted Files

To prevent infected from being opened, Worry-Free Business Security encrypts the file during the following instances:

- Before quarantining a file
- When backing up a file before cleaning it

WFBS provides a tool that decrypts and then restores the file in case you need to retrieve information from it. WFBS can decrypt and restore the following files:

**Table 14-1. Files that WFBS can Decrypt and Restore**

<table>
<thead>
<tr>
<th>FILE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantined files on the client</td>
<td>These files are found in the following directories:</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;Security Agent installation folder&gt;</code>\SUSPECT \Backup</td>
</tr>
<tr>
<td></td>
<td>or <code>&lt;Security Agent installation folder&gt;</code>\quarantine, <strong>whichever is available.</strong></td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;Messaging Security Agent installation folder&gt;</code>\storage\quarantine</td>
</tr>
<tr>
<td></td>
<td>These files are uploaded to the designated quarantine directory, which is typically a directory on the Security Server.</td>
</tr>
</tbody>
</table>
**FILE**

<table>
<thead>
<tr>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantined files on the designated quarantine directory</td>
</tr>
<tr>
<td>By default, this directory is located on the Security Server computer (&lt;Security Server installation folder&gt; \PCCSRV\Virus). To change the directory, navigate to Preferences &gt; Global Settings &gt; System tab and go to the Quarantine Maintenance section.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Backed up encrypted files</th>
</tr>
</thead>
<tbody>
<tr>
<td>These are the backup of infected files that agents were able to clean. These files are found in the following folders:</td>
</tr>
<tr>
<td>• &lt;Security Agent installation folder&gt;\Backup</td>
</tr>
<tr>
<td>• &lt;Messaging Security Agent installation folder&gt;\storage\backup</td>
</tr>
<tr>
<td>To restore these files, users need to move them to the quarantine directory on the client.</td>
</tr>
</tbody>
</table>

---

**WARNING!**

Restoring an infected file may spread the virus/malware to other files and clients. Before restoring the file, isolate the infected client and move important files on this client to a backup location.

---

**Decrypting and Restoring Files on the Security Agent**

**Procedure**

1. Open a command prompt and navigate to <Security Agent installation folder>.

2. Run VSEncode.exe by typing the following:

   ```
   VSEncode.exe /u
   ```

   This parameter opens a screen with a list of files found under <Security Agent installation folder>\SUSPECT\Backup.

3. Select a file to restore and click **Restore**. The tool can only restore one file at a time.
4. In the screen that opens, specify the folder where to restore the file.

5. Click Ok. The file is restored to the specified folder.

**Note**

It might be possible for the agent to scan the file again and treat it as infected as soon as the file is restored. To prevent the file from being scanned, add it to the scan exclusion list. See *Scan Targets and Actions for Security Agents on page 7-8*.

6. Click Close when you have finished restoring files.

---

**Decrypting and Restoring Files on the Security Server,**
**Custom Quarantine Directory, or Messaging Security Agent**

**Procedure**

1. If the file is on the Security Server computer, open a command prompt and navigate to `<Server installation folder>\PCCSRV\Admin\Utility\VSEncrypt`.

   If the file is on a Messaging Security Agent client or a custom quarantine directory, navigate to `<Server installation folder>\PCCSRV\Admin\Utility` and copy the VSEncrypt folder to the client or the custom quarantine directory.

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

   For example, to restore files in `C:\My Documents\Reports`, type `C:\My Documents\Reports\*.*` in the text file.

   Quarantined files on the Security Server computer are found under `<Server installation folder>\PCCSRV\Virus`.

3. Save the text file with an INI or TXT extension. For example, save it as `ForEncryption.ini` on the C: drive.
4. Open a command prompt and navigate to the directory where the VSEncrypt folder is located.

5. Run VSEncode.exe by typing the following:

```plaintext
VSEncode.exe /d /i <location of the INI or TXT file>
```

Where:

- `<location of the INI or TXT file>` is the path of the INI or TXT file you created (for example, `C:\ForEncryption.ini`).

6. Use the other parameters to issue various commands.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (no parameter)</td>
<td>Encrypt files</td>
</tr>
<tr>
<td>/d</td>
<td>Decrypt files</td>
</tr>
<tr>
<td>/debug</td>
<td>Create a debug log and save it to the computer. On the client, the debug log VSEncrypt.log is created in the &lt;Agent installation folder&gt;.</td>
</tr>
<tr>
<td>/o</td>
<td>Overwrite an encrypted or decrypted file if it already exists</td>
</tr>
<tr>
<td>/f &lt;filename&gt;</td>
<td>Encrypt or decrypt a single file</td>
</tr>
<tr>
<td>/nr</td>
<td>Do not restore the original file name</td>
</tr>
<tr>
<td>/v</td>
<td>Display information about the tool</td>
</tr>
<tr>
<td>/u</td>
<td>Launch the tool’s user interface</td>
</tr>
<tr>
<td>/r &lt;Destination folder&gt;</td>
<td>The folder where a file will be restored</td>
</tr>
<tr>
<td>/s &lt;Original file name&gt;</td>
<td>The file name of the original encrypted file</td>
</tr>
</tbody>
</table>

For example, type `VSEncode [/d] [/debug]` to decrypt files in the Suspect folder and create a debug log. When you decrypt or encrypt a file, WFBS creates
the decrypted or encrypted file in the same folder. Before decrypting or encrypting a file, ensure that it is not locked.

Restoring Transport Neutral Encapsulation Format Email Messages

Transport Neutral Encapsulation Format (TNEF) is a message encapsulation format used by Microsoft Exchange/Outlook. Usually this format is packed as an email attachment named Winmail.dat and Outlook Express hides this attachment automatically. See http://support.microsoft.com/kb/241538/en-us.

If the Messaging Security Agent 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.

Using the ReGenID Tool

Each Security Agent installation needs a unique Globally Unique Identifier (GUID) so that the Security Server can identify agents individually. Duplicate GUIDs typically occur on cloned clients or virtual machines.

If two or more agents report the same GUID, run the ReGenID tool to generate a unique GUID for each client.

Procedure

1. On the Security Server, go to the following directory: <Server installation folder>\PCCSRV\Admin\Utility.

2. Copy WFBS_80_WIN_All_ReGenID.exe to a temporary folder on the client where the Security Agent is installed.
   Example: C:\temp

3. Double-click WFBS_80_WIN_All_ReGenID.exe.
   The tool stops the Security Agent and removes the client GUID.
4. Restart the Security Agent.

   The Security Agent generates a new client GUID.

---

**Managing SBS and EBS Add-ins**

Worry-Free Business Security Advanced provides add-ins that allow administrators to view live security and system status information from the consoles of the following Windows operating systems:

- Windows Small Business Server (SBS) 2008
- Windows Essential Business (EBS) Server 2008
- Windows SBS 2011 Standard/Essentials
- Windows Server 2012 Essentials

**Installing the SBS and EBS Add-ins Manually**

The SBS or the EBS add-in installs automatically when you install the Security Server on a computer running Windows SBS 2008, EBS 2008, SBS 2011 Standard/Essentials, or Server 2012 Essentials. To use the add-in on another computer running these operating systems, you need to install it manually.

**Procedure**

1. On the web console, click Preferences > Management Tools and then click the Add-ins tab.

2. Click the corresponding Download link to obtain the installer.

3. Copy and then launch the installer on the target computer.
Using the SBS or EBS Add-ins

Procedure

1. Open the SBS or EBS console.
Appendix A

Security Agent Icons

This appendix explains the different Security Agent icons that display on clients.
Checking the Security Agent Status

The following image shows the Security Agent Console with everything up-to-date and working properly:

![Security Agent Console](image)

The following table lists the icons and their meanings on the Security Agent Console Main User Interface:
### Table A-1. Security Agent Console Main User Interface icons

<table>
<thead>
<tr>
<th>ICON</th>
<th>STATUS</th>
<th>EXPLANATION AND ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Checkmark]</td>
<td>Protection Enabled: You are protected and your software is up to date</td>
<td>The software is up-to-date and running properly. No action is required.</td>
</tr>
<tr>
<td>![X]</td>
<td>Restart Computer: Restart the computer to finish fixing security threats</td>
<td>Security Agent has discovered threats that it cannot fix immediately. Restart the computer to finish fixing these threats.</td>
</tr>
<tr>
<td>![Exclamation]</td>
<td>Protection at Risk: Contact your administrator</td>
<td>Real-time Scan is disabled or protection is at risk for another reason. Enable Real-time Scan and if this does not solve the problem, contact Support.</td>
</tr>
<tr>
<td>![Exclamation]</td>
<td>Update Now: You have not received an update in (number) days.</td>
<td>The virus pattern is older than 3 days. Update the Security Agent immediately.</td>
</tr>
<tr>
<td>![Information]</td>
<td>Smart Scan Not Available: Check your Internet connection</td>
<td>Security Agent has not had access to the Scan Server for over 15 minutes. Ensure you are connected to your network in order to scan with the latest patterns.</td>
</tr>
<tr>
<td>![X]</td>
<td>Restart Computer: Restart your computer to finish installing an update</td>
<td>Restart your computer to finish an update.</td>
</tr>
<tr>
<td>![Information]</td>
<td>Updating Program: Your security software is updating</td>
<td>An update is in progress. Do not disconnect from the network until finished.</td>
</tr>
</tbody>
</table>
Viewing Security Agent Icons on the Windows Task Bar

The following Security Agent icons will display on the client’s Windows Task Bar:

<table>
<thead>
<tr>
<th>ICON</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Status" /></td>
<td>Status is normal</td>
</tr>
<tr>
<td><img src="image" alt="Action" /></td>
<td>(Animated) A Manual Scan or Scheduled Scan is running. The agent is using Conventional Scan or Smart Scan. The Agent is performing an update.</td>
</tr>
<tr>
<td><img src="image" alt="Note" /></td>
<td>Note: Open the Agent Main Console to see what action is required.</td>
</tr>
</tbody>
</table>

Accessing the Console Flyover

The Security Agent Console Flyover will open when hovering your mouse pointer over the small icon on the bottom right of the Security Agent Console.
The following table lists the Console Flyover icons and their meanings:

**Table A-2. Console Flyover Icons**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td><img src="image" alt="Icon" /></td>
<td>Connected to Security Server</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Icon" /></td>
<td>Not connected to Security Server, but real-time scan is still running. The pattern file may not be up to date. Right-click the agent icon in the Windows Task Bar and click <strong>Update Now</strong>.</td>
</tr>
<tr>
<td><strong>Feature</strong></td>
<td><strong>Icon</strong></td>
<td><strong>Meaning</strong></td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Location</td>
<td>![Green Circle]</td>
<td>In Office</td>
</tr>
<tr>
<td></td>
<td>![Gray Circle]</td>
<td>Out of Office</td>
</tr>
<tr>
<td>Real Time Scan</td>
<td>![Green Circle]</td>
<td>On</td>
</tr>
<tr>
<td></td>
<td>![Gray Circle]</td>
<td>Off</td>
</tr>
<tr>
<td>Smart Scan</td>
<td>![Green Circle]</td>
<td>Connected to Scan Server</td>
</tr>
<tr>
<td></td>
<td>![Green Circle]</td>
<td>Connected to Trend Micro Smart Protection Network</td>
</tr>
<tr>
<td></td>
<td>![Gray Circle]</td>
<td>Can’t connect to the Scan Server or Smart Protection Network; protection is reduced as agents are unable to send scan queries.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>![Gray Circle]</td>
</tr>
</tbody>
</table>

- **Firewall**
- **Web Reputation**
- **URL Filtering**
- **Behavior Monitoring**
- **IM Content Filtering**
- **Device Control**

**Note**
Verify that the Smart Scan service TMiCRCScanService is running and that Security Agents are connected to the Security Server.
Appendix B

IPv6 Support in Worry-Free Business Security

This appendix is required reading for users who plan to deploy Worry-Free Business Security in an environment that supports IPv6 addressing. This appendix contains information on the extent of IPv6 support in Worry-Free Business Security.

Trend Micro assumes that the reader is familiar with IPv6 concepts and the tasks involved in setting up a network that supports IPv6 addressing.
IPv6 Support for Worry-Free Business Security

IPv6 support for Worry-Free Business Security started in version 8.0. Earlier Worry-Free Business Security versions do not support IPv6 addressing. IPv6 support is automatically enabled after installing or upgrading the Security Server, Security Agents, and Messaging Security Agents that satisfy the IPv6 requirements.

Security Server IPv6 Requirements

The IPv6 requirements for the Security Server are as follows:

• The server must be installed on Windows Server 2008/2012, SBS 2008/2011, 7, 8, and Vista. It cannot be installed on Windows XP or Server/SBS 2003 because these operating systems only support IPv6 addressing partially.

• The server must use an IIS web server. Apache web server does not support IPv6 addressing.

• If the server will manage IPv4 and IPv6 agents, it must have both IPv4 and IPv6 addresses and must be identified by its host name. If a server is identified by its IPv4 address, pure IPv6 agents cannot connect to the server. The same issue occurs if pure IPv4 clients connect to a server identified by its IPv6 address.

• If the server will manage only IPv6 agents, the minimum requirement is an IPv6 address. The server can be identified by its host name or IPv6 address. When the server is identified by its host name, it is preferable to use its Fully Qualified Domain Name (FQDN). This is because in a pure IPv6 environment, a WINS server cannot translate a host name to its corresponding IPv6 address.

• Verify that the host machine’s IPv6 or IPv4 address can be retrieved using, for example, the “ping” or “nslookup” command.

• If you are installing the Security Server to a pure IPv6 computer, set up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the Security Server and the Internet to allow the server to successfully connect to Trend Micro hosted services, such as the ActiveUpdate server, the Online Registration website, and Smart Protection Network.
Security Agent Requirements

The Security Agent must be installed on:

• Windows Vista (all editions)
• Windows Server 2008 (all editions)
• Windows 7 (all editions)
• Windows SBS 2011
• Windows 8 (all editions)
• Windows Server 2012 (all editions)

It cannot be installed on Windows Server/SBS 2003 and Windows XP because these operating systems only support IPv6 addressing partially.

It is preferable for a Security Agent to have both IPv4 and IPv6 addresses as some of the entities to which it connects only support IPv4 addressing.

Messaging Security Agent Requirements

The Messaging Security Agent (Advanced only) must be installed on a dual-stack or pure IPv6 Microsoft Exchange server.

It is preferable for a Messaging Security Agent to have both IPv4 and IPv6 addresses as some of the entities to which it connects only support IPv4 addressing.

Pure IPv6 Server Limitations

The following table lists the limitations when the Security Server only has an IPv6 address.
**Table B-1. Pure IPv6 Server Limitations**

<table>
<thead>
<tr>
<th>Item</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent management</td>
<td>A pure IPv6 server cannot:</td>
</tr>
<tr>
<td></td>
<td>• Deploy agents to pure IPv4 clients</td>
</tr>
<tr>
<td></td>
<td>• Manage pure IPv4 agents.</td>
</tr>
<tr>
<td>Updates and centralized management</td>
<td>A pure IPv6 server cannot update from pure IPv4 update sources, such as:</td>
</tr>
<tr>
<td></td>
<td>• Trend Micro ActiveUpdate Server</td>
</tr>
<tr>
<td></td>
<td>• Any pure IPv4 custom update source</td>
</tr>
<tr>
<td>Product registration, activation, and</td>
<td>A pure IPv6 server cannot connect to the Trend Micro Online Registration Server to register the product, obtain the license, and activate/renew the license.</td>
</tr>
<tr>
<td>renewal</td>
<td></td>
</tr>
<tr>
<td>Proxy connection</td>
<td>A pure IPv6 server cannot connect through a pure IPv4 proxy server.</td>
</tr>
<tr>
<td>Plug-in solutions</td>
<td>A pure IPv6 server will have Plug-in Manager but will not be able to deploy any of the plug-in solutions to:</td>
</tr>
<tr>
<td></td>
<td>• Pure IPv4 agents or pure IPv4 hosts (because of the absence of a direct connection)</td>
</tr>
<tr>
<td></td>
<td>• Pure IPv6 agents or pure IPv6 hosts because none of the plug-in solutions support IPv6.</td>
</tr>
</tbody>
</table>

Most of these limitations can be overcome by setting up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the Security Server and the entities to which it connects or the entities that it serves.

**Pure IPv6 Agent Limitations**

The following table lists the limitations when agents (Security Agents or Messaging Security Agents) only have an IPv6 address.
### Table B-2. Pure IPv6 Agent Limitations

<table>
<thead>
<tr>
<th>Item</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates</td>
<td>A pure IPv6 agent cannot update from pure IPv4 update sources, such as:</td>
</tr>
<tr>
<td></td>
<td>• Trend Micro ActiveUpdate Server</td>
</tr>
<tr>
<td></td>
<td>• A pure IPv4 Security Server</td>
</tr>
<tr>
<td></td>
<td>• A pure IPv4 Update Agent</td>
</tr>
<tr>
<td></td>
<td>• Any pure IPv4 custom update source</td>
</tr>
<tr>
<td>Scan queries and Smart Feedback</td>
<td>A pure IPv6 Security Agent cannot send queries to Trend Micro Smart Protection Network and cannot use Smart Feedback.</td>
</tr>
<tr>
<td>Proxy connection</td>
<td>A pure IPv6 agent cannot connect through a pure IPv4 proxy server.</td>
</tr>
</tbody>
</table>

Most of these limitations can be overcome by setting up a dual-stack proxy server that can convert between IPv4 and IPv6 addresses (such as DeleGate). Position the proxy server between the agents and the entities to which they connect.

### Configuring IPv6 Addresses

The web console allows you to configure an IPv6 address or an IPv6 address range. The following are some configuration guidelines.

- Worry-Free Business Security accepts standard IPv6 address presentations.

For example:

```
2001:0db7:85a3:0000:0000:8a2e:0370:7334
2001:db7:85a3:0:0:8a2e:370:7334
```
Worry-Free Business Security also accepts link-local IPv6 addresses, such as:

- **2001:db7:85a3::8a2e:370:7334**
- **::ffff:192.0.2.128**
- **fe80::210:5aff:feaa:20a2**

**WARNING!**

Exercise caution when specifying a link-local IPv6 address because even though Worry-Free Business Security can accept the address, it might not work as expected under certain circumstances. For example, agents cannot update from an update source if the source is on another network segment and is identified by its link-local IPv6 address.

- When the IPv6 address is part of a URL, enclose the address in square brackets.
- For IPv6 address ranges, a prefix and prefix length are usually required. For configurations that require the server to query IP addresses, prefix length restrictions apply to prevent performance issues that may occur when the server queries a significant number of IP addresses.
- Some settings that involve IPv6 addresses or address ranges will be deployed to agents but agents will ignore them. For example, if you configured the Update Agent list and included an Update Agent identified by its IPv6 address, pure IPv4 agents will ignore this Update Agent and connect to IPv4 or dual-stack Update Agents, if any.

**Screens That Display IP Addresses**

This topic enumerates places in the web console where IP addresses are shown.

- **Security Groups Tree**

Whenever the Security Groups Tree displays, the IPv6 addresses of pure IPv6 agents display under the **IP address** column. For dual-stack agents, their IPv6 addresses display if they used their IPv6 address to register to the server.
Note

The IP address that dual-stack agents use when registering to the server can be controlled in the Preferred IP Address section in Preferences > Global Settings > Desktop/Server tab.

When you export agent settings to a file, the IPv6 addresses also display in the exported file.

- Logs

The IPv6 addresses of dual-stack and pure IPv6 agents display on the logs.
Appendix C

Getting Help

This appendix describes how to get help, find additional information, and contact Trend Micro.
The Trend Micro Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro website, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:


Trend Micro updates the contents of the Knowledge Base continuously and adds new solutions daily. If you are unable to find an answer, however, you can describe the problem in an email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

Contacting Technical Support

Before contacting Trend Micro Technical Support it is recommended that you run the Case Diagnostic Tool first (See Case Diagnostic Tool on page C-3).

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

• Technical Support:

• Submit a Support Case Online:

• If you prefer to communicate by email message, send a query to the following address:
  support@trendmicro.com

• In the United States, you can also call the following toll-free telephone number:
  (877) TRENDAV, or 877-873-6328
• Trend Micro product documentation:
  

### Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) collects necessary debugging information from a customer’s product whenever problems occur. It automatically turns the product's debug status on and off and collects necessary files according to problem categories. Trend Micro uses this information to troubleshoot problems related to the product.


### Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

### Contact Information

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:
Sending Suspicious Files to Trend Micro

If you think you have an infected file but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send in the suspicious file.

You can also send Trend Micro the URL of any website you suspect of being a phish site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and viruses).

• Send an email to virusresponse@trendmicro.com, and specify "Phish or Disease Vector" as the Subject.
• Use the Trend Micro Anti-Threat Toolkit:


Security Information Center

Comprehensive security information is available at the Trend Micro website:

• List of viruses and malicious mobile code currently "in the wild," or active
• Computer virus hoaxes
• Internet threat advisories
• Virus weekly report
• Threat Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
Getting Help


• Glossary of terms

TrendLabs

TrendLabs℠ is the global antivirus research and support center of Trend Micro. Located on three continents, TrendLabs has a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

• Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
• Emergency virus outbreak support
• Email access to antivirus engineers
• Knowledge Base, the Trend Micro online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

Product Terminology and Concepts

The items contained in this appendix provide further information about Trend Micro products and technologies.
Hot Fix

A hot fix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes do not (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).

By default, the Security Agents can install hot fixes. If you do not want Security Agents to install hot fixes, change update settings in the web console by going to Security Settings > {Group} > Configure > Client Privileges. Under Update Privileges, select Disable Security Agent upgrade and hot fix deployment.

IntelliScan

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

Using IntelliScan provides the following benefits:

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

IntelliTrap

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

---

**Note**

IntelliTrap uses the same scan engine as virus scanning. As a result, the file handling and scanning rules for IntelliTrap are the same as administrator-defined rules for virus scanning.

Agents write bot and other malware detections to the IntelliTrap log. You can export the contents of the IntelliTrap log for inclusion in reports.

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

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap 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 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 potentially dangerous. These technologies can reduce, by as much as two-thirds, the number of files the scan engine examines; this file-scanning reduction also creates some risk that a harmful file might be allowed onto the network.

For example, .gif files make up a large volume of all web traffic, but they are unlikely to harbor viruses/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.

Intrusion Detection System

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

- **Too Big Fragment**: A Denial of Service attack where a hacker directs an oversized TCP/UDP packet at a target computer. This can cause the computer's buffer to overflow, which can freeze or reboot the computer.

- **Ping of Death**: A Denial of Service attack where a hacker directs an oversized ICMP/ICMPv6 packet at a target computer. This can cause the computer's buffer to overflow, which can freeze or reboot the computer.

- **Conflicted ARP**: A type of attack where a hacker sends an Address Resolution Protocol (ARP) request with the same source and destination IP address to a computer. The target computer continually sends an ARP response (its MAC address) to itself, causing it to freeze or crash.

- **SYN Flood**: A Denial of Service attack where a program sends multiple TCP synchronization (SYN) packets to a computer, causing the computer to continually send synchronization acknowledgment (SYN/ACK) responses. This can exhaust computer memory and eventually crash the computer.

- **Overlapping Fragment**: Similar to a Teardrop attack, this Denial of Service attack sends overlapping TCP fragments to a computer. This overwrites the header information in the first TCP fragment and may pass through a firewall. The firewall may then allow subsequent fragments with malicious code to pass through to the target computer.

- **Teardrop**: Similar to an overlapping fragment attack, this Denial of Service attack deals with IP fragments. A confusing offset value in the second or later IP fragment can cause the receiving computer's operating system to crash when attempting to reassemble the fragments.
• **Tiny Fragment Attack**: A type of attack where a small TCP fragment size forces the first TCP packet header information into the next fragment. This can cause routers that filter traffic to ignore the subsequent fragments, which may contain malicious data.

• **Fragmented IGMP**: A Denial of Service attack that sends fragmented IGMP packets to a target computer, which cannot properly process the IGMP packets. This can freeze or slow down the computer.

• **LAND Attack**: A type of attack that sends IP synchronization (SYN) packets with the same source and destination address to a computer, causing the computer to send the synchronization acknowledgment (SYN/ACK) response to itself. This can freeze or slow down the computer.

Keywords

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

• Words (guns, bombs, and so on)
• Numbers (1,2,3, and so on)
• Special characters (&,#,+ , and so on)
• Short phrases (blue fish, red phone, big house, and so on)
• Words or phrases connected by logical operators (apples .AND. oranges)
• Words or phrases that use regular expressions (.REG. a.*e matches “ace”, “ate”, and “advance”, but not “all”, “any”, or “antivirus”)

WFBS can import an existing list of keywords from a text (.txt) file. Imported keywords appear in the keyword list.

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 D-1. Using Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>How It Works</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>any keyword</td>
<td>The Messaging Security Agent searches content that matches the word</td>
<td>Type the word and add it to the keyword list</td>
</tr>
<tr>
<td>OR</td>
<td>The Messaging Security Agent searches for any of the keywords separated by OR</td>
<td>Type &quot;<strong>.OR.</strong>&quot; between all the words you want to include For example, &quot;apple .OR. orange&quot;</td>
</tr>
<tr>
<td>AND</td>
<td>The Messaging Security Agent searches for all of the keywords separated by AND</td>
<td>Type &quot;<strong>.AND.</strong>&quot; between all the words you want to include For example, &quot;apple .AND. orange&quot;</td>
</tr>
<tr>
<td>NOT</td>
<td>The Messaging Security Agent excludes keywords following NOT from search.</td>
<td>Type &quot;<strong>.NOT.</strong>&quot; before a word you want to exclude For example, &quot;<strong>.NOT. juice</strong>&quot;</td>
</tr>
</tbody>
</table>
### Product Terminology and Concepts

<table>
<thead>
<tr>
<th>Operator</th>
<th>How it Works</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>WILD</td>
<td>The wildcard symbol replaces a missing part of the word. Any words that are spelled using the remaining part of the wildcard are matched.</td>
<td>Type <code>.WILD.</code> before the parts of the word you want to include. For example, if you want to match all words containing “valu”, type <code>.WILD.valu</code>. The words Valumart, valucash, and valubucks all match.</td>
</tr>
</tbody>
</table>

Note:
The Messaging Security Agent does not support using “?” in the wildcard command “.WILD.”.

| REG      | To specify a regular expression, add a .REG. operator before that pattern (for example, .REG. a.*e). See [Regular Expressions on page D-9](#) | Type `.REG.` before the word pattern you want to detect. For example, `.REG. a.*e` matches: “ace”, “ate”, and “advance”, but not “all”, “any”, nor “antivirus”. |

### Using Keywords Effectively

The Messaging Security Agent offers simple and powerful features to create highly specific filters. Consider the following when creating your Content Filtering rules:

- By default, the Messaging Security Agent searches for exact matches of keywords. Use regular expressions to search for partial matches of keywords. See [Regular Expressions on page D-9](#).
- The Messaging Security Agent 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 the following table for more information about using keywords on multiple lines.
- You can also set the Messaging Security Agent to search for synonyms of the actual keywords.
<table>
<thead>
<tr>
<th>SITUATION</th>
<th>EXAMPLE</th>
<th>MATCH/NON-MATCH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two words on same line</td>
<td>guns bombs</td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Click here to buy guns bombs and other weapons.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Click here to buy guns and bombs.”</td>
</tr>
<tr>
<td>Two words separated by a comma</td>
<td>guns, bombs</td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Click here to buy guns, bombs, and other weapons.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Click here to buy used guns, new bombs, and other weapons.”</td>
</tr>
<tr>
<td>Multiple words on multiple lines</td>
<td>guns</td>
<td>When you choose <strong>Any specified keywords</strong></td>
</tr>
<tr>
<td></td>
<td>bombs</td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td>weapons and</td>
<td>“Guns for sale”</td>
</tr>
<tr>
<td></td>
<td>ammo</td>
<td>Also matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Buy guns, bombs, and other weapons”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you choose <strong>All specified keywords</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Buy guns bombs weapons and ammo”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Buy guns bombs weapons ammunition.”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Also does not match:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>“Buy guns, bombs, weapons, and ammo”</td>
</tr>
</tbody>
</table>
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”

### Patch

A patch is 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, while non-Windows patches commonly have a setup script.

### Regular Expressions

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

There are a number of websites and tutorials available online. One such site is the PerlDoc site, which can be found at:


**WARNING!**

Regular expressions are a powerful string matching tool. For this reason, Trend Micro recommends that Administrators who choose to use regular expressions be familiar and comfortable with regular expression syntax. Poorly written regular expressions can have a dramatic negative performance impact. Trend Micro recommends is to start with simple regular expressions that do not use complex syntax. When introducing new rules, use the archive action and observe how the Messaging Security Agent manages messages using your rule. When you are confident that the rule has no unexpected consequences, you can change your action.
Regular Expression Examples

See the following tables for some common examples of regular expressions. To specify a regular expression, add a “.REG.” operator before that pattern.

**Table D-3. Counting and Grouping**

<table>
<thead>
<tr>
<th><strong>Element</strong></th>
<th><strong>What it Means</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>The dot or period character represents any character except new line character.</td>
<td>do. matches doe, dog, don, dos, dot, etc. d.r matches deer, door, etc.</td>
</tr>
<tr>
<td>*</td>
<td>The asterisk character means zero or more instances of the preceding element.</td>
<td>do* matches d, do, doo, dooo, doooo, etc.</td>
</tr>
<tr>
<td>+</td>
<td>The plus sign character means one or more instances of the preceding element.</td>
<td>do+ matches do, doo, dooo, doooo, etc. but not d</td>
</tr>
<tr>
<td>?</td>
<td>The question mark character means zero or one instances of the preceding element.</td>
<td>do?g matches dg or dog but not doog, dooog, etc.</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis characters group whatever is between them to be considered as a single entity.</td>
<td>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.”</td>
</tr>
</tbody>
</table>
## Product Terminology and Concepts

### Table D-4. Character Classes (shorthand)

<table>
<thead>
<tr>
<th><strong>ELEMENT</strong></th>
<th><strong>WHAT IT MEANS</strong></th>
<th><strong>EXAMPLE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>Square bracket characters indicate a set or a range of characters.</td>
<td>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.</td>
</tr>
<tr>
<td>[ ^ ]</td>
<td>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.</td>
<td>d[^aeiouy] matches db, dc or dd, d9, d#--d followed by any single character except a vowel.</td>
</tr>
<tr>
<td>{ }</td>
<td>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.</td>
<td>da{3} matches daaa--d followed by 3 and only 3 occurrences of “a”. da{2,4} matches daa, daaa, daaaa, and daaaaa (but not daaaaaa)--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”.</td>
</tr>
<tr>
<td>\d</td>
<td>Any digit character; functionally equivalent to [0-9] or [[:digit:]]</td>
<td>\d matches 1, 12, 123, etc., but not 1b7--one or more of any digit characters.</td>
</tr>
<tr>
<td><strong>ELEMENT</strong></td>
<td><strong>WHAT IT MEANS</strong></td>
<td><strong>EXAMPLE</strong></td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>\D</td>
<td>Any non-digit character; functionally equivalent to [^0-9] or [^[:digit:]]\</td>
<td>\D matches a, ab, ab&amp;, but not 1--one or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.</td>
</tr>
<tr>
<td>\w</td>
<td>Any “word” character--that is, any alphanumeric character; functionally equivalent to [^_A-Za-z0-9] or [^[:alnum:]]\</td>
<td>\w matches a, ab, a1, but not !&amp;--one or more upper- or lower-case letters or digits, but not punctuation or other special characters.</td>
</tr>
<tr>
<td>\W</td>
<td>Any non-alphanumeric character; functionally equivalent to [^^_A-Za-z0-9] or [^^[:alnum:]]\</td>
<td>\W matches *, &amp;, but not ace or a1--one or more of any character but upper- or lower-case letters and digits.</td>
</tr>
<tr>
<td>\s</td>
<td>Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [[:space]]</td>
<td>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.</td>
</tr>
<tr>
<td>\S</td>
<td>Any non-white space character; anything other than a space, new line, tab, non-breaking space, etc.; functionally equivalent to [^[:space]]</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Table D-5. Character Classes**

<table>
<thead>
<tr>
<th><strong>ELEMENT</strong></th>
<th><strong>WHAT IT MEANS</strong></th>
<th><strong>EXAMPLE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>[:alpha:]</td>
<td>Any alphabetic characters</td>
<td>.REG. [:alpha:] matches abc, def, xxx, but not 123 or @$$.</td>
</tr>
<tr>
<td>[:digit:]</td>
<td>Any digit character; functionally equivalent to \d</td>
<td>.REG. [:digit:] matches 1, 12, 123, etc.</td>
</tr>
<tr>
<td>ELEMENT</td>
<td>WHAT IT MEANS</td>
<td>EXAMPLE</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[:alnum:]</td>
<td>Any “word” character—that is, any alphanumeric character; functionally equivalent to \w</td>
<td>.REG. [:alnum:] matches abc, 123, but not ~!@.</td>
</tr>
<tr>
<td>[:space:]</td>
<td>Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to \s</td>
<td>.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.</td>
</tr>
<tr>
<td>[:graph:]</td>
<td>Any characters except space, control characters or the like</td>
<td>.REG. [:graph:] matches 123, abc, xxx, &lt;&gt;, but not space or control characters.</td>
</tr>
<tr>
<td>[:print:]</td>
<td>Any characters (similar with [:graph:]) but includes the space character</td>
<td>.REG. [:print:] matches 123, abc, xxx, &lt;&gt;, and space characters.</td>
</tr>
<tr>
<td>[:cntrl:]</td>
<td>Any control characters (e.g. CTRL + C, CTRL + X)</td>
<td>.REG. [:cntrl:] matches 0x03, 0x08, but not abc, 123, !@#.</td>
</tr>
<tr>
<td>[:blank:]</td>
<td>Space and tab characters</td>
<td>.REG. [:blank:] matches space and tab characters, but not 123, abc, !@#</td>
</tr>
<tr>
<td>[:punct:]</td>
<td>Punctuation characters</td>
<td>.REG. [:punct:] matches ; : ? ! ~ @ # $ % &amp; * ’ “ , etc., but not 123, abc</td>
</tr>
<tr>
<td>[:lower:]</td>
<td>Any lowercase alphabetic characters (Note: ‘Enable case sensitive matching’ must be enabled or else it will function as [:alnum:])</td>
<td>.REG. [:lower:] matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, ! @#.</td>
</tr>
</tbody>
</table>
| [: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 D-6. Pattern Anchors

<table>
<thead>
<tr>
<th>Element</th>
<th>What it Means</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Indicates the beginning of a string.</td>
<td>^(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.</td>
</tr>
<tr>
<td>$</td>
<td>Indicates the end of a string.</td>
<td>(notwithstanding)$ 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.</td>
</tr>
</tbody>
</table>

### Table D-7. Escape Sequences and Literal Strings

<table>
<thead>
<tr>
<th>Element</th>
<th>What it Means</th>
<th>Example</th>
</tr>
</thead>
</table>
| \      | 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 ?. |
<p>| \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. |</p>
<table>
<thead>
<tr>
<th><strong>ELEMENT</strong></th>
<th><strong>WHAT IT MEANS</strong></th>
<th><strong>EXAMPLE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>\n</td>
<td>Indicates a new line character.</td>
<td>(stress)\n\n matches any block of text that contained the substring “stress” followed immediately by two new line (ASCII 0x0A) characters.</td>
</tr>
<tr>
<td>Note</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>\r</td>
<td>Indicates a carriage return character.</td>
<td>(stress)\r matches any block of text that contained the substring “stress” followed immediately by one carriage return (ASCII 0x0D) character.</td>
</tr>
<tr>
<td><strong>ELEMENT</strong></td>
<td><strong>WHAT IT MEANS</strong></td>
<td><strong>EXAMPLE</strong></td>
</tr>
<tr>
<td>-------------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>\b</td>
<td>Indicates a backspace character. OR Denotes boundaries.</td>
<td>(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</td>
</tr>
<tr>
<td>\xhh</td>
<td>Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).</td>
<td>\x7E(\w){6} matches any block of text containing a “word” of exactly six alphanumeric characters preceded with a ~ (tilde) character. So, the words ‘~ab12cd’, ‘~Pa3499’ would be matched, but ‘~oops’ would not.</td>
</tr>
</tbody>
</table>

**Regular Expression Generator**

When deciding how to configure rules for Data Loss Prevention, consider that the regular expression generator can create only simple expressions according to the following rules and limitations:

- Only alphanumeric characters can be variables.
- All other characters, such as [-], [/], and so on can only be constants.
- Variable ranges can only be from A-Z and 0-9; you cannot limit ranges to, say, A-D.
• Regular expressions generated by this tool are case-insensitive.

• Regular expressions generated by this tool can only make positive matches, not negative matches (“if does not match”).

• Expressions based on your sample can only match the exact same number of characters and spaces as your sample; the tool cannot generate patterns that match “one or more” of a given character or string.

**Complex Expression Syntax**

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

Operators include .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., “." and “.\.” The operand and the operator must be separated by a space. An operand may also contain several tokens. See *Keywords on page D-5*.

**Regular Expressions at Work**

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 expression matches with the social security number. The following table describes the strings that match the example regular expression:

**TABLE D-8. Numbers Matching the Social Security Regular Expression**

<table>
<thead>
<tr>
<th>.REG. \b\d{3}-\d{2}-\d{4}\b</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>333-22-4444</td>
<td>Match</td>
</tr>
<tr>
<td>3332244444</td>
<td>Not a match</td>
</tr>
<tr>
<td>333 22 4444</td>
<td>Not a match</td>
</tr>
<tr>
<td>3333-22-4444</td>
<td>Not a match</td>
</tr>
</tbody>
</table>
If you modify the expression as follows,

\[\text{Format} \text{.REG.} \backslash b \backslash d \{3\} \backslash x20 \backslash d \{2\} \backslash x20 \backslash d \{4\} \backslash b\]

the new expression matches the following sequence:

333 22 4444

### Scan Exclusion Lists

#### Scan Exclusion List for Security Agents

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

**TABLE D-9. Security Agent Exclusion List**

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Installation Path Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>InterScan eManager 3.5x</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>ProgramDirectory=</td>
</tr>
<tr>
<td>ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>ProgramDirectory=</td>
</tr>
<tr>
<td>ScanMail for Lotus Notes (SMLN) eManager NT</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>AppDir=</td>
</tr>
<tr>
<td></td>
<td>DataDir=</td>
</tr>
<tr>
<td></td>
<td>IniDir=</td>
</tr>
<tr>
<td><strong>PRODUCT NAME</strong></td>
<td><strong>INSTALLATION PATH LOCATION</strong></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InterScan Web Security Suite (IWSS)</td>
<td>HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite</td>
</tr>
<tr>
<td></td>
<td>Program Directory= C:\Program Files\Trend Micro\IWSS</td>
</tr>
<tr>
<td>InterScan WebProtect</td>
<td>HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>ProgramDirectory=</td>
</tr>
<tr>
<td>InterScan FTP VirusWall</td>
<td>HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>ProgramDirectory=</td>
</tr>
<tr>
<td>InterScan Web VirusWall</td>
<td>HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>ProgramDirectory=</td>
</tr>
<tr>
<td>InterScan E-Mail VirusWall</td>
<td>HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>ProgramDirectory=(Installation Drive):\INTERS-1</td>
</tr>
<tr>
<td>InterScan NSAPI Plug-In</td>
<td>HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>ProgramDirectory=</td>
</tr>
<tr>
<td>InterScan E-Mail VirusWall</td>
<td>HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>ProgramDirectory=</td>
</tr>
<tr>
<td><strong>PRODUCT NAME</strong></td>
<td><strong>INSTALLATION PATH LOCATION</strong></td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IM Security (IMS)</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>HomeDir=</td>
</tr>
<tr>
<td></td>
<td>VSQuarantineDir=</td>
</tr>
<tr>
<td></td>
<td>VSBackupDir=</td>
</tr>
<tr>
<td></td>
<td>FBArchiveDir=</td>
</tr>
<tr>
<td></td>
<td>FTCFArchiveDir=</td>
</tr>
<tr>
<td><strong>Product Name</strong></td>
<td><strong>Installation Path Location</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>ScanMail for Microsoft Exchange (SMEX)</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>TempDir=</td>
</tr>
<tr>
<td></td>
<td>DebugDir=</td>
</tr>
<tr>
<td></td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption</td>
</tr>
<tr>
<td></td>
<td>BackupDir=</td>
</tr>
<tr>
<td></td>
<td>MoveToQuarantineDir=</td>
</tr>
<tr>
<td></td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder=</td>
</tr>
<tr>
<td></td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption</td>
</tr>
<tr>
<td></td>
<td>BackupDir=</td>
</tr>
<tr>
<td></td>
<td>MoveToQuarantineDir=</td>
</tr>
<tr>
<td></td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption \Advance QuarantineFolder=</td>
</tr>
<tr>
<td><strong>PRODUCT NAME</strong></td>
<td><strong>INSTALLATION PATH LOCATION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------</td>
</tr>
</tbody>
</table>
| ScanMail for Microsoft Exchange (SMEX) | HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption  
BackupDir=  
MoveToQuarantineDir=  
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager  
QMDir=  
Get exclusion.txt file path from HKEY_LOCAL_MACHINE \SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange \CurrentVersion\HomeDir  
Go to HomeDir path (for example, C:\Program Files \Trend Micro\Messaging Security Agent)  
Open exclusion.txt  
C:\Program Files\Trend Micro\Messaging Security Agent\Temp\  
C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\  
C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\  
C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\  
C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool |

**Scan Exclusion Lists for Messaging Security Agent (Advanced Only)**

By default, when the Messaging Security Agent is installed on a Microsoft Exchange server (2000 or later) it will not scan Microsoft Exchange databases, Microsoft Exchange log files, Virtual server folders, or the M:\ drive. The exclusion list is saved in:
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

ExcludeExchangeStoreFiles=C:\Program Files\Exchsrvr\mdbdata\priv1.stm|C:\Program Files\Exchsrvr\mdbdata\priv1.edb|C:\Program Files\Exchsrvr\mdbdata\pub1.stm|C:\Program Files\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Program Files\Exchsrvr\mdbdata\|C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue\|C:\Program Files\Exchsrvr\Mailroot\vsi 1\PickUp\|C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail\

For other Microsoft Exchange recommended folders, please add them to scan exclusion list manually. See http://support.microsoft.com/kb/245822/.

**SBS 2003 Exclusions**

For SBS 2003, manually add the following:

<table>
<thead>
<tr>
<th>Microsoft Exchange exclusions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange Server Database</td>
<td>C:\Program Files\Exchsrvr\MDBDATA</td>
</tr>
<tr>
<td>Microsoft Exchange MTA files</td>
<td>C:\Program Files\Exchsrvr\Mtadata</td>
</tr>
<tr>
<td>Microsoft Exchange Message tracking log files</td>
<td>C:\Program Files\Exchsrvr\server_name.log</td>
</tr>
<tr>
<td>Microsoft Exchange SMTP Mailroot</td>
<td>C:\Program Files\Exchsrvr\Mailroot</td>
</tr>
<tr>
<td>Microsoft Exchange working files</td>
<td>C:\Program Files\Exchsrvr\MDBDATA</td>
</tr>
<tr>
<td>Site Replication Service</td>
<td>C:\Program Files\Exchsrvr\srsdata</td>
</tr>
<tr>
<td></td>
<td>C:\Program Files\Exchsrvr\conndata</td>
</tr>
<tr>
<td>IIS Exclusions</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>IIS System Files</td>
<td>C:\WINDOWS\system32\inetsrv</td>
</tr>
<tr>
<td>IIS Compression Folder</td>
<td>C:\WINDOWS\IIS Temporary Compressed Files</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain Controller Exclusions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory database files</td>
<td>C:\WINDOWS\NTDS</td>
</tr>
<tr>
<td>SYSVOL</td>
<td>C:\WINDOWS\SYSVOL</td>
</tr>
<tr>
<td>NTFRS Database Files</td>
<td>C:\WINDOWS\ntfrs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows SharePoint Services Exclusions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary SharePoint folder</td>
<td>C:\windows\temp\FrontPageTempDir</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client Desktop Folder Exclusions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Update Store</td>
<td>C:\WINDOWS\SoftwareDistribution\DataStore</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Additional Exclusions</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removable Storage Database (used by SBS Backup)</td>
<td>C:\Windows\system32\NtmsData</td>
</tr>
<tr>
<td>SBS POP3 connector Failed Mail</td>
<td>C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Failed Mail</td>
</tr>
<tr>
<td>SBS POP3 connector Incoming Mail</td>
<td>C:\Program Files\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail</td>
</tr>
<tr>
<td>Windows Update Store</td>
<td>C:\WINDOWS\SoftwareDistribution\DataStore</td>
</tr>
<tr>
<td>DHCP Database Store</td>
<td>C:\WINDOWS\system32\dhcp</td>
</tr>
</tbody>
</table>
Security Patch

A security patch focuses on security issues suitable for deployment to all customers. Windows security patches include a Setup program, while non-Windows patches commonly have a setup script.

Service Pack

A service pack is 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.

Trojan Port

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

**Table D-10. Trojan Ports**

<table>
<thead>
<tr>
<th>PORT NUMBER</th>
<th>TROJAN HORSE PROGRAM</th>
<th>PORT NUMBER</th>
<th>TROJAN HORSE PROGRAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>23432</td>
<td>Asylum</td>
<td>31338</td>
<td>Net Spy</td>
</tr>
<tr>
<td>31337</td>
<td>Back Orifice</td>
<td>31339</td>
<td>Net Spy</td>
</tr>
<tr>
<td>18006</td>
<td>Back Orifice 2000</td>
<td>139</td>
<td>Nuker</td>
</tr>
<tr>
<td>12349</td>
<td>Bionet</td>
<td>44444</td>
<td>Prosiak</td>
</tr>
<tr>
<td>6667</td>
<td>Bionet</td>
<td>8012</td>
<td>Ptakks</td>
</tr>
<tr>
<td>PORT NUMBER</td>
<td>TROJAN HORSE PROGRAM</td>
<td>PORT NUMBER</td>
<td>TROJAN HORSE PROGRAM</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------</td>
<td>-------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>80</td>
<td>Codered</td>
<td>7597</td>
<td>Qaz</td>
</tr>
<tr>
<td>21</td>
<td>DarkFTP</td>
<td>4000</td>
<td>RA</td>
</tr>
<tr>
<td>3150</td>
<td>Deep Throat</td>
<td>666</td>
<td>Ripper</td>
</tr>
<tr>
<td>2140</td>
<td>Deep Throat</td>
<td>1026</td>
<td>RSM</td>
</tr>
<tr>
<td>10048</td>
<td>Delf</td>
<td>64666</td>
<td>RSM</td>
</tr>
<tr>
<td>23</td>
<td>EliteWrap</td>
<td>22222</td>
<td>Rux</td>
</tr>
<tr>
<td>6969</td>
<td>GateCrash</td>
<td>11000</td>
<td>Senna Spy</td>
</tr>
<tr>
<td>7626</td>
<td>Gdoor</td>
<td>113</td>
<td>Shiver</td>
</tr>
<tr>
<td>10100</td>
<td>Gift</td>
<td>1001</td>
<td>Silencer</td>
</tr>
<tr>
<td>21544</td>
<td>Girl Friend</td>
<td>3131</td>
<td>SubSari</td>
</tr>
<tr>
<td>7777</td>
<td>GodMsg</td>
<td>1243</td>
<td>Sub Seven</td>
</tr>
<tr>
<td>6267</td>
<td>GW Girl</td>
<td>6711</td>
<td>Sub Seven</td>
</tr>
<tr>
<td>25</td>
<td>Jesrto</td>
<td>6776</td>
<td>Sub Seven</td>
</tr>
<tr>
<td>25685</td>
<td>Moon Pie</td>
<td>27374</td>
<td>Sub Seven</td>
</tr>
<tr>
<td>68</td>
<td>Mspy</td>
<td>6400</td>
<td>Thing</td>
</tr>
<tr>
<td>1120</td>
<td>Net Bus</td>
<td>12345</td>
<td>Valvo line</td>
</tr>
<tr>
<td>7300</td>
<td>Net Spy</td>
<td>1234</td>
<td>Valvo line</td>
</tr>
</tbody>
</table>

**Uncleanable Files**

This topic discusses files that Security Agents and Messaging Security Agents are unable to clean.
Uncleanable by the Security Agent

The Security Agent is unable to clean the following files:

**Table D-11. Uncleanable Files**

<table>
<thead>
<tr>
<th><strong>Uncleanable File</strong></th>
<th><strong>Explanation and Solution</strong></th>
</tr>
</thead>
</table>
| Files infected with Trojans | Trojans are programs that perform unexpected or unauthorized, usually malicious, actions such as displaying messages, erasing files, or formatting disks. Trojans do not infect files, thus cleaning is not necessary.  
**Solution:** The Security Agent uses the Virus Cleanup Engine and Virus Cleanup Template to remove Trojans. |
| Files infected with Worms | A computer worm is a self-contained program (or set of programs) able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments. Worms are uncleanable because the file is a self-contained program.  
**Solution:** Trend Micro recommends deleting worms. |
| Write-protected infected files | **Solution:** Remove the write-protection to allow the Security Agent to clean the file. |
| Password-protected files | Includes password-protected compressed files or password-protected Microsoft Office files.  
**Solution:** Remove the password protection for the agent to clean these files. |
| Backup files | Files with the RB0~RB9 extensions are backup copies of infected files. The Security Agent creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.  
**Solution:** If the Security Agent successfully cleans the infected file, you do not need to keep the backup copy. If the computer functions normally, you can delete the backup file. |
### Uncleanable File

<table>
<thead>
<tr>
<th><strong>Infected files in the Recycle Bin</strong></th>
<th><strong>Explanation and Solution</strong></th>
</tr>
</thead>
</table>
| The Security Agent may not remove infected files in the Recycle Bin because the system is running. | **Solution on Windows XP or Windows Server 2003 with NTFS File System:**
1. Log on to the computer with Administrator privilege.
2. Close all running applications to prevent applications from locking the file, which would make Windows unable to delete it.
3. Open the command prompt, and type the following to delete the files:
   ```
   cd \\
   cd recycled
   del *.* /S
   ```
   The last command deletes all files in the Recycle Bin.
4. Check if the files were removed. |
<p>| <strong>Infected files in Windows Temp Folder or Internet Explorer Temporary Folder</strong> | The Security Agent may not clean infected files in the Windows Temp folder or the Internet Explorer temporary folder because the computer uses them. The files to clean may be temporary files needed for Windows operation. |</p>
<table>
<thead>
<tr>
<th><strong>UNCLEANABLE FILE</strong></th>
<th><strong>EXPLANATION AND SOLUTION</strong></th>
</tr>
</thead>
</table>

**Solution on Windows XP or Windows Server 2003 with NTFS File System:**

1. Log on to the computer with Administrator privilege.

2. Close all running applications to prevent applications from locking the file, which would make Windows unable to delete it.

3. If the infected file is in the Windows Temp folder:
   a. Open the command prompt and go to the Windows Temp folder (located at `C:\Windows\Temp` for Windows XP or Windows Server 2003 computers by default).
   b. Type the following to delete the files:
      ```
      cd temp
      attrib -h
      del *.* /S
      ```
      The last command deletes all files in the Windows Temp folder.

4. If the infected file is in the Internet Explorer temporary folder:
   a. Open a command prompt and go to the Internet Explorer Temp folder (located in `C:\Documents and Settings\<Your user name>\Local Settings\Temporary Internet Files` for Windows XP or Windows Server 2003 computers by default).
   b. Type the following to delete the files:
      ```
      cd tempor~1
      attrib -h
      del *.* /S
      ```
      The last command deletes all files in the Internet Explorer temporary folder.

   c. Check if the files were removed.
### UNCLEANABLE FILE

<table>
<thead>
<tr>
<th>Solution on other operating systems (or those without NTFS):</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Restart the computer in MS-DOS mode.</td>
</tr>
<tr>
<td>2. If the infected file is in the Windows Temp folder:</td>
</tr>
<tr>
<td>a. At the command prompt, go to the Windows Temp folder. The default Windows Temp folder in Windows XP or Windows Server 2003 is C:\Windows\Temp.</td>
</tr>
<tr>
<td>b. Open the command prompt, and type the following to delete the files:</td>
</tr>
<tr>
<td>cd temp</td>
</tr>
<tr>
<td>attrib -h</td>
</tr>
<tr>
<td>del <em>.</em> /S</td>
</tr>
<tr>
<td>The last command deletes all files in the Windows Temp folder.</td>
</tr>
<tr>
<td>c. Restart the computer in normal mode.</td>
</tr>
<tr>
<td>3. If the infected file is in the Internet Explorer temporary folder:</td>
</tr>
<tr>
<td>a. At the command prompt, go to the Internet Explorer temporary folder. The default Internet Explorer temporary folder in Windows XP or Windows Server 2003 is C:\Documents and Settings&lt;Your user name&gt;\Local Settings\Temporary Internet Files.</td>
</tr>
<tr>
<td>b. Type the following commands:</td>
</tr>
<tr>
<td>cd tempor~1</td>
</tr>
<tr>
<td>attrib -h</td>
</tr>
<tr>
<td>del <em>.</em> /S</td>
</tr>
<tr>
<td>The last command deletes all files in the Internet Explorer temporary folder.</td>
</tr>
<tr>
<td>c. Restart the computer in normal mode.</td>
</tr>
</tbody>
</table>
### Uncleanable File

<table>
<thead>
<tr>
<th>Uncleanable File</th>
<th>Explanation and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files compressed using an unsupported compression format</td>
<td><strong>Solution</strong>: Uncompress the files.</td>
</tr>
<tr>
<td>Locked files or files that are currently executing</td>
<td><strong>Solution</strong>: Unlock the files or wait until the files have been executed.</td>
</tr>
<tr>
<td>Corrupted files</td>
<td><strong>Solution</strong>: Delete the files.</td>
</tr>
</tbody>
</table>

### Uncleanable by the Messaging Security Agent (Advanced only)

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

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

- The file contains a Trojan, worm, or other malicious code. To stop an executable from executing, the Messaging Security Agent must completely remove it.

- The Messaging Security Agent does not support all compression forms. The scan engine only cleans files compressed using pkzip and only when the infection is in the first layer of compression.

- An unexpected problem prevents the Messaging Security Agent from cleaning, such as:
  - The temp directory that acts as a repository for files requiring cleaning is full
    - The file is locked or is currently executing.
    - The file is corrupted.
    - The file is password protected.
Index

A
ActiveAction, 7-14
ActiveX malicious code, 1-9
AutoPcc.exe, 3-8, 3-9, 3-13

B
Behavior Monitoring Configuration Pattern, 8-8
Behavior Monitoring Core Service, 8-8
Behavior Monitoring Detection Pattern, 8-7
Behavior Monitoring Driver, 8-8
boot sector virus, 1-9

C
Case Diagnostic Tool, C-3
client installation
Client Packager, 3-14
from the web console, 3-18
Login Script Setup, 3-13
using Vulnerability Scanner, 3-21
Client Packager, 3-9, 3-14, 3-16
deployment, 3-17
settings, 3-15
COM file infector, 1-9
Common Firewall Driver, 8-7
Common Firewall Pattern, 1-9
component duplication, 8-10
components, 8-3
Conflicted ARP, D-4
contacting, C-2–C-5
documentation feedback, C-5
Knowledge Base, C-2
sending suspicious files, C-4
technical support, C-2
Trend Micro, C-2–C-5
conventional scan, 5-3, 5-4

D
Damage Cleanup Engine, 8-7
Damage Cleanup Services, 3-4
DHCP settings, 3-24
Digital Signature Pattern, 8-8
documentation, xii
documentation feedback, C-5

E
EICAR test script, 1-9
encrypted files, 14-9
EXE file infector, 1-9
external device protection, 8-8

F
file reputation, 1-4
firewall
benefits, 5-9
Fragmented IGMP, D-5

H
hot fixes, 8-9
HTML virus, 1-10

I
IDS, D-4
incremental pattern, 8-10
IntelliTrap Exception Pattern, 8-6
IntelliTrap Pattern, 8-6
Intrusion Detection System, D-4
IPv6 support, B-2
displaying IPv6 addresses, B-6
limitations, B-3, B-4
**J**  
Java malicious code, 1-9  
JavaScript virus, 1-10  
joke program, 1-8

**K**  
Knowledge Base, C-2

**L**  
LAND Attack, D-5  
Login Script Setup, 3-8, 3-9, 3-13

**M**  
macro virus, 1-9

**N**  
network virus, 1-9, 5-10  
new features, 1-2

**O**  
Overlapping Fragment, D-4

**P**  
packer, 1-9  
patches, 8-9  
Ping of Death, D-4  
Plug-in Manager, 3-5  
Policy Enforcement Pattern, 8-8  
pre-installation tasks, 3-11, 3-18, 3-21  
probable virus/malware, 1-8  
programs, 8-3

**Q**  
quarantine directory, 5-28, 14-10

**R**  
remote installation, 3-9  
rootkit detection, 8-8

**S**  
scan actions  
spyware/grayware, 7-13  
scan method, 3-15  
scan types, 3-3  
Security Agent installation methods, 3-8  
Security Information Center, C-4  
security patches, 8-9  
security risks, 1-10, 1-11  
spyware/grayware, 1-10, 1-11

server update  
component duplication, 8-10  
manual update, 8-12  
scheduled update, 8-13  
smart protection, 1-3, 1-4  
File Reputation Services, 1-4  
Smart Protection Network, 1-3  
Web Reputation Services, 1-4

Smart Protection Network, 1-3  
smart scan, 5-3, 5-4  
spyware/grayware, 1-10, 1-11  
adware, 1-10  
dialers, 1-10  
hacking tools, 1-10  
joke programs, 1-10  
password cracking applications, 1-11  
remote access tools, 1-10  
spyware, 1-10

spyware/grayware scan actions, 7-13  
Spyware Pattern, 8-7  
Spyware Scan Engine, 8-7  
suspicious files, C-4  
SYN Flood, D-4

**T**  
Teardrop, D-4
technical support, C-2
test virus, 1-9
Tiny Fragment Attack, D-5
Too Big Fragment, D-4
TrendLabs, C-5
Trend Micro
contact information, C-3
Knowledge Base, C-2
Security Information Center, C-4
TrendLabs, C-5
Trojan horse program, 1-8, 8-7

U
uninstallation
using the uninstallation program, 3-40
Update Agent, 3-5

V
VBScript virus, 1-10
virus/malware, 1-8–1-10
  ActiveX malicious code, 1-9
  boot sector virus, 1-9
  COM and EXE file infector, 1-9
  Java malicious code, 1-9
  joke program, 1-8
  macro virus, 1-9
  packer, 1-9
  probable virus/malware, 1-8
  test virus, 1-9
  Trojan horse program, 1-8
  types, 1-8–1-10
  VBScript, JavaScript or HTML virus,
  1-10
  worm, 1-10
Virus Cleanup Template, 8-7
Virus Encyclopedia, 1-8
Virus Pattern, 8-6, 8-14
Virus Scan Engine, 8-5
Vulnerability Scanner, 3-10, 3-21
  computer description retrieval, 3-29
  DHCP settings, 3-24
  ping settings, 3-30
W
web console, 2-4, 2-5
  about, 2-4
  requirements, 2-5
web install page, 3-8
web reputation, 1-4, 3-4
WFBS
  components, 8-3
  documentation, xii
  worm, 1-10