9.0

Worry-Free™
Business Security
Standard and Advanced Editions
Service Pack 2
Administrator's Guide

Securing Your Journey to the Cloud

Protected Cloud   **Web Security**

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

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

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.

Document Part No.: WFEM97026/150706

Release Date: July 2015

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

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

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.

Evaluate this documentation on the following site:

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

Table of Contents

Preface

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

Chapter 2: Getting Started

Chapter 3: Installing Agents

Chapter 4: Managing Groups

Chapter 5: Managing Basic Security Settings for Security Agents

Chapter 6: Managing Basic Security Settings for Messaging Security Agents (Advanced Only)

Chapter 7: Managing Scans

Chapter 8: Managing Updates

Chapter 9: Managing Notifications

Chapter 10: Using Outbreak Defense

Chapter 11: Managing Global Settings

Chapter 12: Using Logs and Reports

Chapter 13: Performing Administrative Tasks

Chapter 14: Using Management Tools

Appendix A: Security Agent Icons

Appendix B: IPv6 Support in WFBS

Appendix C: Getting Help

Appendix D: Product Terminology and Concepts

Index

Preface

Preface

Welcome to the Trend Micro™ Worry-Free™ Business Security *Administrator's Guide*. This document discusses getting started information, agent installation procedures, and Security Server and agent management.

Worry-Free Business Security Documentation

Worry-Free Business Security documentation includes the following:

TABLE 1. Worry-Free Business Security Documentation

DOCUMENTATION	DESCRIPTION
Installation and Upgrade Guide	A PDF document that discusses requirements and procedures for installing the Security Server, and upgrading the server and agents
Administrator's Guide	A PDF document that discusses getting started information, client installation procedures, and Security Server and agent management
Help	HTML files compiled in WebHelp or CHM format that provide "how to's", usage advice, and field-specific information
Readme file	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
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com

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

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

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

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

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 (WFBS 9.0 SP2)

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

TABLE 1-1. What's New in WFBS 9.0 SP2

FEATURE/ENHANCEMENT	DESCRIPTION
Windows 10 support	Worry-Free Business Security now supports Security Agent installation on Windows 10.
Ransomware Protection for documents	Enhanced scan features can identify and block ransomware programs that target documents that run on endpoints by identifying common behaviors and blocking processes commonly associated with ransomware programs.

TABLE 1-2. Resolved Known Issues

ITEM NO.	HOT FIX/ CRITICAL PATCH NUMBER	ISSUE	SOLUTION
1	B2363	The Security Agent may still protect Intuit files after the user disables the Intuit QuickBooks Protection function.	This hot fix ensures that users can disable the Intuit Quickbooks Protection function successfully.
2	B2363	The Security Agent may still protect folders after the user disables the folder protection function.	This hot fix ensures that users can disable the folder protection function successfully.
3	B2453	When starting the Worry-Free Business Security 9.0 Service Pack 1 Agent with POP3 email scanning enabled, the Real-time Scan (Ntrtscan.exe) service may not be able to start due to a timing conflict with the Trend Micro Security Agent Listener (TmListen.exe) service.	This critical patch resolves the timing conflict by ensuring that the Trend Micro Security Agent Listener service allows the RealTime Scan service to start before starting other services.
4	B2453	On some environments, part of the scanning process may hang and the Worry-Free Business Security 9.0 Service Pack 1 Agent may be unable to perform any action on the detected malware. When this happens, Worry-Free Business Security does not display a pop-up warning or generate a detection log.	This critical patch enables Worry-Free Business Security 9.0 Service Pack 1 Agent to perform the required action on malware detected under the scenario described above.
5	B2479	The Manual Scan progress window stops responding during a manual scan.	This hot fix ensures that manual scans run and completes normally.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
6	B2500	An issue prevents Worry-Free Business Security 9.0 Service Pack 1 servers from updating the Smart Scan Pattern successfully. When this happens, the live status of the Smart Scan Service on the server's web console becomes "unavailable".	This hot fix ensures that Worry-Free Business Security 9.0 Service Pack 1 servers can update the Smart Scan Pattern successfully.
7	B2502	An issue prevents Worry-Free Business Security 9.0 Service Pack 1 servers from disabling the global setting: "Send Web Reputation and URL Filtering Logs to the Security Server".	This hot fix ensures that Worry-Free Business Security 9.0 Service Pack 1 servers can disable the setting "Send Web Reputation and URL Filtering Logs to the Security Server".
8	B2503	On Microsoft(TM) 64-bit operating systems, the 32-bit version of Internet Explorer 9 might crash when it coexists with the Security Agent.	This hot fix ensures that this browser works fine when it coexists with the Security Agent on Microsoft 64-bit operating systems.
9	B2510	The SMTP mail scan feature is enabled by default when the Worry-Free Business Security 9.0 Service Pack 1 agent is installed on the Microsoft(TM) Windows(TM) 8.0, 8.1, or Server 2012 R2 platform. When this happens, both the platform's email server and client may not be able to send or receive some email messages.	This hot fix ensures that the Security Agent works well with the platform email server and client.

ITEM No.	HOT FIX/ CRITICAL PATCH NUMBER	ISSUE	SOLUTION
10	B2514	Users may encounter performance issues on computers where the Worry-Free Business Security 9.0 Service Pack 1 Agent is installed.	This hot fix resolves the performance issues on affected computers.
11	B2515	An issue related to the "coreTaskManager.dll" binary file may trigger a heap leak issue after the Worry-Free Business Security 9.0 Service Pack 1 Agent is installed on the computer.	This hot fix resolves the heap leak issue on affected computers.
12	B2516	Users may be unable to install the Trend Micro Remote Manager agent on computers where the Worry-Free Business Security 9.0 Service Pack 1 server is installed. When this happens, users will be unable to register Worry-Free Business Security to the Trend Micro Remote Manager using its existing GUID.	This hot fix resolves the installation issues to ensure that users can install the Trend Micro Remote Manager agent on computers where the Worry-Free Business Security 9.0 Service Pack 1 server is installed.
13	B2517	Computers where the Worry-Free Business Security 9.0 Service Pack 1 Agent is installed may stop responding after the Real-time Scan feature is enabled.	This hot fix ensures that the Real-time Scan feature Worry-Free Business Security 9.0 Service Pack 1 Agents works normally.
14	B2519	Users may encounter system crash problems when installing the Worry-Free Business Security 9.0 Service Pack 1 Agent.	This hot fix resolves the system crash issues when installing the Worry-Free Business Security 9.0 Service Pack 1 Agent.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
15	B2520	Sometimes, Worry-Free Business Security 9.0 Service Pack 1 cannot detect a USB disk device that has been ejected from and plugged back into a protected computer.	This hot fix ensures that Worry-Free Business Security 9.0 Service Pack 1 can detect USB disk devices that are plugged into protected computers.
16	B2534	Users may encounter system crash problems after installing the Worry-Free Business Security 9.0 Service Pack 1 Agent.	This hot fix resolves the system crash issues when installing the Worry-Free Business Security 9.0 Service Pack 1 Agent.
17	B2541	Worry-Free Business Security 9.0 Service Pack 1 may stop unexpectedly or trigger blue screen of death (BSOD) in a Microsoft™ Windows™ Server environment with a Cluster Shared Volumes (CSV) disk.	This hot fix ensures that Worry-Free Business Security 9.0 Service Pack 1 works well with CSV disks within a Windows Server Failover Cluster.

What's New in WFBS 9.0 SP1

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

TABLE 1-3. What's New in WFBS 9.0 SP1

Feature/Enhancement	Description
Detection improvements	• Outbreak prevention protection against compressed executable files (packers) • Improved Damage Cleanup Engine performance

Feature/Enhancement	Description
Enhancements	Web reputation logs include running processes information
Usability improvements	• Security Server version displays on the log on screen • Updated UI text to better reflect how WFBS works

Table 1-4. Resolved Known Issues

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
1	N/A	A user requests for a way to configure the Messaging Security Agent to run attachment-blocking scans on quarantined spam email messages (MSA 11.1.1254).	This hot fix adds an option to configure the Messaging Security Agent to run attachment-blocking scans on quarantined spam email messages.
2	1433	After upgrading Worry-Free Business Security server from version 8.0 or 8.0 Service Pack 1 to 9.0, the live status of the Smart Scan Service on the server web console becomes "unavailable". This occurs because Worry-Free Business Security 9.0 server cannot update the Smart Scan pattern successfully.	This hot fix ensures that the Worry-Free Business Security 9.0 server can update the Smart Scan Pattern successfully.
3	1439	The Worry-Free Business Security 9.0 server package contains an OpenSSL cryptographic software library that is affected by the Heartbleed vulnerability.	This critical patch updates the OpenSSL cryptographic software library in the Worry-Free Business Security 9.0 SP1 server package to resolve this issue.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
4	1440	If Microsoft™ Windows™ is in high-contrast mode and users access the Worry-Free Business Security 9.0 console in Microsoft Internet Explorer, users will not be able to move clients from one group to another.	This hot fix corrects a function attribute to enable Internet Explorer to properly retrieve information when Windows is in high-contrast mode. This helps ensure that users can successfully move clients between groups under this scenario.
5	1442	Worry-Free Business Security Agents may not be able to run manual scans on network drives.	This hot fix ensures that Worry-Free Business Security Agents can run manual scans on network drives.
6	1445	Worry-Free Business Security server database process may encounter memory leak during Spyware log query.	This hot fix ensures that the Worry-Free Business Security Server database process does not encounter memory leak when doing Spyware log query.
7	1451	When users sort data by clicking the "Viruses Detected", "Spyware Detected", "Spam Detected", and "URLs Violated" columns in the client tree of the server user interface, Worry-Free Business Security cannot sort the data correctly.	This hot fix corrects the data sorting issue that affects the "Viruses Detected", "Spyware Detected", "Spam Detected", and "URLs Violated" columns.
8	1452	Security Agent services fail to load during startup if administrators use the AutoPCC login script for deploying clients.	This hot fix ensures that the Security Agent services work properly during startup if administrators use the AutoPCC login script for deploying clients.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
9	1454	Users randomly get pop-up windows from the Security Agent for no apparent reason.	This hot fix ensures that users only receive pop-up windows from the Security Agent for necessary events based on their notification configuration.
10	1456	On Microsoft™ 64-bit operating systems (OS), the 32-bit version of Internet Explorer 9 might crash when it coexists with the Security Agent.	This hot fix ensures that this browser works fine when it coexists with the Security Agent on Microsoft 64-bit operating systems.
11	1457	The "Action Taken" field in virus logs that were exported from the Worry-Free Business Security Server does not contain any information.	This hot fix ensures that virus logs are imported properly from the Worry-Free Business Security Server.
12	1458	There is an inconsistency in the "Date/Time" field between the POP3 mail log of Worry-Free Business Security Server and the log of Security Agent.	This hot fix ensures that information in POP3 mail log of Worry-Free Business Security Server will be consistent with the log of Security Agent.
13	1459	Users may not be able to update the Smart Scan Pattern from an HTTP redirection source.	This hot fix ensures that the update procedure can correctly process the dollar sign character in HTTP redirection responses so users can successfully update the Smart Scan Pattern from an HTTP redirection source.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
14	1459	Security Agents receive balloon notifications when the agent is updating its program files. Customer's requesting a way to disable this type of balloon notification.	This hot fix provides an option to disable the balloon notification that appears when the agent is upgrading its program files.
15	1466	After installing the Worry-Free Business Security Agent, process PccNTMon.exe may encounter a handle leak issue.	This hot fix resolves the handle leak issue on affected computers.
16	2062	The EYES driver that comes with the Worry-Free Business Security package and works with a third-party driver may sometimes report false positives.	This hot fix updates the EYES driver to help prevent it from reporting false positives.
17	2063	TmListen might stop unexpectedly after Worry-Free Business Security Agent installation.	This hot fix ensures that the TmListen run successfully after Worry-Free Business Security Agent installation.
18	5215	The Security Agent installed on computers running Windows XP cannot detect malware located in the boot sector of a USB device when users log on Windows with a non-administrator account.	This hot fix updates Security Agent files to resolve this issue.
19	5215	The Ntrtscan.exe service may stop unexpectedly while the Security Agent performs a manual scan on a location with a path length that exceeds 260 characters.	This hot fix enables Security Agent to use a flexible variable instead of a fixed variable to store file paths during scans to prevent Ntrtscan.exe from stopping unexpectedly.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
20	5215	Sometimes, the Security Agent Listener service, TmListen.exe, stops unexpectedly while the Security Agent starts up.	This hot fix enhances Security Agent's error-handling mechanism to prevent TmListen.exe from stopping unexpectedly while Security Agent start up.
21	5215	Sometimes, the status of an Security Agent computer appears as "Trend Micro Security Agent is turned off" on the Microsoft™ Windows™ Action Center even the Security Agent is enabled on the computer.	This hot fix updates the Security Agent files to ensure that the correct Security Agent status appears on the Windows Action Center.
22	5227	It may take a long time to log on to the Security Agent console in the Novell™ ZENworks™ Application platform because of an issue in the Virus Scan Engine settings.	This hot fix resolves this issue by allowing users to modify the Virus Scan Engine settings in the Worry-Free Business Security server and to globally deploy the new Virus Scan Engine settings to Worry-Free Business Security clients.
23	5238	The Security Server cgiCheckIP.exe function allows users to scan any port inside any network.	This hot fix enhances the port-checking mechanism of the cgiCheckIP.exe function to enable it to properly validate the port number sent from a client before scanning the port.
24	5245	Microsoft™ Office™ hangs when opening Office files in shared folders. This issue can be solved with deploy the CheckRtPCWOplock parameter.	This hot fix enables users to set the following CheckRtPCWOplock parameter in the **Global Setting** and deploy to the client to fix the hang issue.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
25	5248	Sometimes, the status of a Security Agent computer in a VPN network environment appears as "Trend Micro Security Agent is turned off" on the Microsoft™ Windows™ Action Center.	This hot fix updates the Security Agent files to ensure that the correct client status appears on the Windows Action Center.
26	5248	Security Agent always overwrites this client registry key and sets it as the default value for the firewall module: HKLM\SYSTEM\CurrentControlSet\services\tmtdi\Parameters\RedirectIpv6	This hot fix modifies the Redirect IPv6 function by manually (but not forcibly) overwriting the RedirectIpv6 key, setting it as default value.
27	5274	During Security Agent updates, Security Agent retrieves the Other Update Sources (OUS) settings from the ClientAllSetting.ini file and updates the OUS.ini file using the retrieved information. However, when the Security Server Master Service stops, the "ClientAllSetting.ini" file is cleared. As a result, Security Agent will not be able to retrieve any OUS settings to update the OUS.ini file which can cause Security Agent updates to fail.	This hot fix adds a checking mechanism that prevents Security Agentt from making changes to the OUS.ini file if it cannot retrieve any OUS settings from the ClientAllSetting.ini file. This ensures that Security Agents can still complete updates when the ClientAllSetting.ini file is empty.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
28	5339	Sometimes, the Virus Cleanup Template version on the Security Agent console becomes "0" after the client updates the template and loads the new version.	This hot fix enhances the version-checking mechanism to ensure that the correct Virus Cleanup Template version appears on the Security Agent console.
29	5350	Users may not be able to access internal web sites when the Security Agent uses IPv6 to redirect URLs to Web Reputation Service (WRS).	This hot fix resolves the issue by providing an option to configure Security Agents to redirect URLs to WRS using IPv4 instead of IPv6 and to deploy the setting globally.
30	5366	Microsoft™ Outlook™ stops responding when launched on computers running the Security Agent Behavior Monitoring service.	Hotfix provide deploy the Behavior Monitoring settings that can prevent Outlook from stopping unexpectedly in this situation.
31	5369	The Security Agent does not generate a spyware log when it detects spyware in a self-extracting compressed file and all its actions on the file fail.	This hot fix ensures that Security Agent generates spyware logs when it detects spyware in a compressed file and all its actions on the file fail.
32	5390	The Security Agent's OUS.ini file becomes truncated after an update. This happens when the OUS.ini file is larger than the allotted memory buffer for the copy function which forces the function to truncate the file to fit the buffer.	This hot fix increases the memory buffer for the OUS.ini copy function to prevent the function from truncating the OUS.ini file of Security Agents during updates.

Item No.	Hot Fix/ Critical Patch Number	Issue	Solution
33	5399	Sometimes, the Virus Cleanup Template version on the OfficeScan client console becomes "0" after the client updates the template and loads the new version.	This hot fix enhances the version-checking mechanism to ensure that the correct Virus Cleanup Template version appears on the OfficeScan client console.
34	5443	The rollback process for Smart Scan Agent and virus pattern files may not work correctly.	This hot fix ensures that the rollback process for Smart Scan Agent and virus pattern files work correctly.
35	5463	A third-party software may stop responding on a Security Agent computer when both the client's Unauthorized Change Prevention Service and Firewall Services are enabled.	This hot fix enables users to deploy a firewall setting to prevent third-party software from stopping unexpectedly on Security Agent computers when both the client's Unauthorized Change Prevention Service and Firewall Services are enabled.
36	5485	When a Security Agent performs a manual scan and the scan path is longer that 63 characters, the corresponding scan log does not appear in the "Virus Logs" viewer.	This hot fix ensures that the scan logs are recorded successfully when the scan path is longer than 63 characters.
37	5492	Security Agents installed on 64-bit platforms may not be able to update from the update agent.	This hot fix ensures that Security Agents will update successfully from update agents.
38	5495	Some components may not be updated when its modules are used by some features during Security Agent update.	This fix ensures that all components are updated during Security Agent update.

What's New in WFBS 9.0

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

TABLE 1-5. What's New in WFBS 9.0

FEATURE/ENHANCEMENT	DESCRIPTION
Microsoft Exchange support	WFBS now supports Microsoft Exchange Server 2010 SP3 and Microsoft Exchange Server 2013.
Windows support	WFBS now supports Microsoft Windows 8.1 and Windows Server 2012 R2.

Mobile device security	WFBS Advanced now supports mobile device data protection and access control. Mobile device security has the following features:
	
	• Device Access Control
	
	    • Allow access to the Exchange server based on user, operating system, and / or email client
	
	    • Specify the access granted to specific mailbox components
	
	• Device Management
	
	    • Perform a device wipe on lost or stolen devices
	
	    • Apply security settings to specific users including:
	
	        • Password strength requirements
	
	        • Automatic device lock after being inactive
	
	        • Encryption
	
	        • Unsuccessful sign-in data purge

Activation Code enhancement	Post-paid Activation Code support

FEATURE/ENHANCEMENT	DESCRIPTION
Detection improvements	• Enhanced Memory Scan for real-time scan • Known and potential threat mode for Behavior Monitoring • Browser Exploit Prevention • Newly encountered program download detection
Performance improvements	• Installation and un-installation time of Security Agent • Deferred Scan for Real-time Scan
Usability improvements	• Global and group Approval/Block lists for Web Reputation and URL Filtering • IP exception list for Web Reputation and URL Filtering in the Global Settings • Removal of ActiveX from Client Tree and Remote installation page • Customized Outbreak Defense • Outlook 2013 and Windows Live Mail 2012 support for Trend Micro Anti-Spam Toolbar • Update Agent to update from Trend Micro ActiveUpdate only • Stop Server updates • Keep patterns when upgrading the Server and Agent • Help Link and Infection Source virus logs

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 agents 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 clients. 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 1-6. Benefits of Protection

THREAT	PROTECTION
Virus/Malware. Virus, Trojans, Worms, Backdoors, and Rootkits **Spyware/Grayware**. Spyware, Dialers, Hacking tools, Password cracking applications, Adware, Joke programs, and Keyloggers	File-based scans (Real-time Scan, Manual Scan, Scheduled Scan)
Security threats transmitted through email messages	**POP3 Mail Scan** in the Security Agent
Network worms/viruses and intrusions	Firewall in the Security Agent
Conceivably harmful websites/Phishing sites	Web Reputation and URL Filtering in the Security Agent
Security threats that spread through USB and other external devices	Device Control in the Security Agent
Malicious behavior	Behavior Monitoring in the Security Agent

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:

  http://about-threats.trendmicro.com/threatencyclopedia.aspx

- **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.

    - **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

Endpoints 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 clients 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 client 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:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

TYPE	DESCRIPTION
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 client Internet settings and can force the client 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 client 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.
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 networks or clients either by force or without permission. It could also mean bypassing the security of a network or client.

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.

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 Content to Trend Micro on page C-3* for more information.

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 client, 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 client 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

AGENT	DESCRIPTION
Security Agent	Protects desktops and servers from security threats and intrusions
Messaging Security Agent (Advanced only)	Protects Microsoft Exchange servers from email-borne security threats

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.

- Configure product settings 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 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 7.0 or later

*   High-color display with a resolution of 1024x768 or higher

*   Microsoft Edge on HTTPS channel

> **Tip**
>
> Messaging Security Agent server console does not support Windows 10 Microsoft Edge browser.
>
> Use Internet Explorer 7 or later if you encounter any problems when accessing the console using the Edge browser.

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 the computer that hosts the Security Server, click **Windows Start menu** > **Trend Micro Worry-Free Business Security** > **Worry-Free Business Security**.

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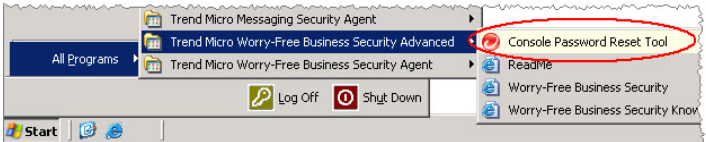
The browser displays the Worry-Free Business Security logon screen.

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.

ITEM TO CHECK	DETAILS
Password	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.
Browser Cache	If you upgraded from a previous version of WFBS, web browser and proxy server cache files may prevent the web console from loading. Clear the cache memory on your browser and on any proxy servers located between the Trend Micro Security Server and the client you use to access the web console.

Item To Check	Details
SSL Certificate	Verify that your web server is functioning properly. If you are using SSL, verify that the SSL certificate is still valid. See your web server documentation for details.

Virtual Directory Settings	There may be a problem with the virtual directory settings if you are running the web console on an IIS server and the following message appears:
	
	`The page cannot be displayed`
	
	`HTTP Error 403.1 - Forbidden: Execute access is denied.`
	
	`Internet Information Services (IIS)`
	
	This message may appear when either of the following addresses is used to access the console:
	
	http://{server name}/SMB/
	
	http://{server name}/SMB/default.htm
	
	However, the console may open without any problems when using the following address:
	
	http://{server name}/SMB/console/html/cgi/cgichkmasterpwd.exe
	
	To resolve this issue, check the execute permissions of the SMB virtual directory.
	
	To enable scripts:
	
	1. Open the Internet Information Services (IIS) manager.
	
	2. In the SMB virtual directory, select **Properties**.
	
	3. Select the Virtual Directory tab and change the execute permissions to `scripts` instead of `none`. Also, change the execute permissions of the client install virtual directory.

Web Console Navigation

Web Console Main Sections

The web console contains the following main sections:

SECTION	DESCRIPTION
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 Settings**, 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:

Menu Options	Description
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	Configure and deploy Outbreak Defense, Vulnerability Assessment, and Damage Cleanup.
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	Description
Preferences	• Set up notifications for abnormal threat-related or system-related events • Set up global settings for ease of maintenance • Use management tools to help manage security for the network and clients • View product license information, maintain the administrator password, and help keep the business environment safe for the exchange of digital information by joining the Smart Feedback program
Help	• Search for specific content and topics • View the Administrator's Guide • Access the latest information from the Knowledge Base (KB) • View Security, Sales, Support, and version information

Web Console Icons

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

Table 2-2. Web Console Icons

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

Live Status

Use the **Live Status** screen to get an overall view of the threat security of your network.

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

Understanding Icons

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

TABLE 2-3. Live Status Icons

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

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

Threat Status

This section shows the following information:

TABLE 2-4. Threat Status Sections and Displayed Information

SECTION	DESCRIPTION
Outbreak Defense	A possible virus outbreak on your network.

Section	Description
Antivirus	Configured from the notification, the status icon changes to display the Warning icon. If you must take action: • 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. • Real-time scanning is disabled on Security Agents. Click **Enable Now** to start Real-time scanning again. • Real-time scanning is disabled on the Messaging Security Agent.
Anti-spyware	Displays the latest spyware scan results and spyware log entries. The **Number of Incidents** column of the Spyware Threat Incidents table displays the results of the latest spyware scan. To find more information about specific clients, click the number link under the **Incidents Detected** column of the Spyware Threat Incidents table. From there, you can find information about the specific spyware threats that are affecting your clients.
Anti-spam	Click the **High**, **Medium**, or **Low** link to be redirected to the configuration screen for the selected Microsoft Exchange server where you can set the threshold level from the Anti-spam screen. Click **Disabled** to be redirected to the appropriate screen. This information is updated on an hourly basis.
Web Reputation	Potentially dangerous websites as determined by Trend Micro.
URL Filtering	Restricted websites as determined by the administrator.
Behavior Monitoring	Violations of the behavior monitoring policies.
Network Viruses	Detections determined by the firewall settings.

Section	Description
Device Control	Restricts access to USB devices and network drives

> **Note**
>
> WFBS supports all kinds of storage devices that connect through a USB interface, except smartphones and digital cameras.

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

Section	Description
Component Updates	The status of component updates for the deployment of updated components to agents.
Smart Scan	The Security Agents that cannot connect to the Scan Server. **Note** The Scan Server is a service hosted on the Security Server.
Unusual system events	Disk space information about clients that are functioning as servers (running server operating systems).

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

ITEM	UPDATE INTERVAL (MINUTES)	AGENT SENDS LOGS TO SERVER AFTER... (MINUTES)
Outbreak Defense	3	N/A
Antivirus	1	Security Agent: Immediate Messaging Security Agent: 5
Anti-spyware	3	1
Anti-spam	3	60
Web Reputation	3	Immediate
URL Filtering	3	Immediate
Behavior Monitoring	3	2
Network Viruses	3	2
Device Control	3	2
Smart Scan	60	N/A
License	10	N/A
Component Updates	3	N/A
Unusual System Events	10	When the listening service TmListen is started

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:

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

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.

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 5-21*.

    - **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

FEATURE	WINDOWS OPERATING SYSTEM								
	XP	VISTA	7	8/8.1	10	SERVER/SBS 2003	SERVER/SBS 2008	SERVER 2008 R2/SBS 2011	SERVER 2012/R2
Manual Scan, Real-time Scan, and Scheduled Scan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Web reputation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
URL Filtering	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Behavior Monitoring	Yes (32-bit) No (64-bit)	Yes (32/64-bit) No (64-bit without SP1)	Yes	Yes	Yes	Yes (32-bit) No (64-bit)	Yes	Yes	Yes
Device Control	Yes (32-bit) No (64-bit)	Yes (32/64-bit) No (64-bit without SP1)	Yes	Yes	Yes	Yes (32-bit) No (64-bit)	Yes	Yes	Yes

FEATURE	WINDOWS OPERATING SYSTEM								
	XP	VISTA	7	8/8.1	10	SERVER/SBS 2003	SERVER/SBS 2008	SERVER 2008 R2/SBS 2011	SERVER 2012/R2
Damage Cleanup Services	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
POP3 mail scan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Manual and scheduled updates	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Update Agent	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Agent Plug-in Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Smart Feedback	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

FEATURE	WINDOWS OPERATING SYSTEM								
	XP	VISTA	7	8/8.1	10	SERVER/SBS 2003	SERVER/SBS 2008	SERVER 2008 R2/SBS 2011	SERVER 2012/R2
Trend Micro Anti-spam Toolbar	Yes (32-bit) No (64-bit)	Yes	Yes	Yes	Yes	No	No	No	No
	Supported email clients: • Microsoft Outlook 2003 (32-bit), 2007 (32-bit), 2010 (32- and 64-bit), 2013 (32- and 64-bit) • Outlook Express 6.0 with Service Pack 2 or later • Windows Mail 6.0 • Windows Live Mail 2011, 2012								
HouseCall	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Case Diagnostic Tool	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wi-Fi Advisor	Yes	Yes	Yes	Yes	Yes	No	No	No	No

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 2008/2008 R2 (all editions)

- Windows 7 (all editions)

- Windows SBS 2008/2011

- Windows 8/8.1 (all editions)

- Windows 10 (all editions)

- Windows Server 2012/2012 R2 (all editions)

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

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

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

INSTALLATION METHOD	REQUIREMENTS/CONSIDERATIONS
Internal Web Page and Email Notification Install	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 **Preferred IP Address** section in **Preferences** > **Global Settings** > **Desktop/Server** tab.

INSTALLATION METHOD	REQUIREMENTS/CONSIDERATIONS
Vulnerability Scanner and Remote Install	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.

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 pure IPv6 client can manage pure IPv6 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

INSTALLATION METHOD/ OPERATING SYSTEM SUPPORT	DEPLOYMENT CONSIDERATIONS					
	WAN DEPLOYMENT	CENTRALLY MANAGED	REQUIRES USER INTERVENTION	REQUIRES IT RESOURCE	MASS DEPLOYMENT	BANDWIDTH CONSUMED
Internal Web Page Supported on all operating systems	Yes	Yes	Yes	No	No	Low, if scheduled
Email Notification Supported on all operating systems	Yes	Yes	Yes	No	No	High, if installations start at the same time
Remote Install Supported on all operating systems except: • Windows Vista Home Basic and Home Premium Editions • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 Basic • Windows 10 Home	No	Yes	No	Yes	Yes	Low, if scheduled

INSTALLATION METHOD/ OPERATING SYSTEM SUPPORT	DEPLOYMENT CONSIDERATIONS					
	WAN DEPLOYMENT	CENTRALLY MANAGED	REQUIRES USER INTERVENTION	REQUIRES IT RESOURCE	MASS DEPLOYMENT	BANDWIDTH CONSUMED
Login Script Setup Supported on all operating systems	No	Yes	No	Yes	Yes	High, if installations start at the same time
Client Packager Supported on all operating systems	Yes	No	Yes	Yes	No	Low, if scheduled
Trend Micro Vulnerability Scanner (TMVS) Supported on all operating systems except: • Windows Vista Home Basic and Home Premium Editions • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 Basic • Windows 10 Home	No	Yes	No	Yes	Yes	Low, if scheduled

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, 8.1, Server 2003/2008/2008 R2/2012/2012 R2, or SBS 2003/2008/2011 • with Internet Information Server (IIS) 6.0, 7.0, 7.5, 8.0, 8.5, or Apache 2.0.6x
Target client	• The target client must have Internet Explorer 7.0 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).

ITEM TO CHECK	REQUIREMENT
Target client running Windows XP, 7, 8, 8.1, 10, Vista, Server 2003, 2008, 2008 R2, 2012, 2012 R2, or SBS 2003, 2008, 2011	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 3-32*.

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

PACKAGE TYPE	DESCRIPTION
Setup	Select **Setup** 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.
Update	Select **Update** 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.

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, 8/8.1, 10, Server 2008, SBS 2011, Server 2012, or Server 2012 R2 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 3-38*.

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:

ITEM TO CHECK	REQUIREMENT
Target client	• Use an administrator account to log on to each target 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). • 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.
Target client running Windows Vista, 7, 8/8.1, 10, Server 2008,	Perform the following tasks:

ITEM TO CHECK	REQUIREMENT
2012/2012 R2, or SBS 2011	**Note** When performing remote installation on Windows 8/8.1 or 10, the Microsoft account cannot be used to login to the target client
	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. Disable User Account Control.
	Note For Windows 8/8.1, 10, or 2012/2012 R2: Modify the following registry key to turn off User Account Control: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] "EnableLUA"=dword:00000000.
	3. Temporarily start the Remote Registry service.
	a. Open Microsoft Management Console.
	Note Type `services.msc` in the Run window to open Microsoft Management Console.

ITEM TO CHECK	REQUIREMENT
	b. Right-click **Remote Registry** and select **Start**.
	4. If required, return to the original settings after installing Security Agents on the Windows Vista, 7, 8/8.1, or 10 client.
Target client running Windows XP	On the client, temporarily disable Simple File Sharing: 1. Open Windows Explorer. 2. Click **Tools** > **Folder Options**. 3. On the View tab, clear **Use Simple File Sharing (Recommended)**. 4. Click **Apply**.
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 Computer**.

    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 **Status** 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 of 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:

ITEM TO CHECK	REQUIREMENT
Where to launch Vulnerability Scanner	You can launch Vulnerability Scanner on the Security Server or on any client in the network. The client should not be running Terminal Server.

ITEM TO CHECK	REQUIREMENT
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

Run vulnerability scans on demand.

Procedure

1. Launch Vulnerability Scanner.

TO LAUNCH VULNERABILITY SCANNER ON:	STEPS
The Security Server	a. **Navigate to** <Server installation folder>\PCCSRV\Admin \Utility\TMVS. b. **Double-click** TMVS.exe.

To Launch Vulnerability Scanner On:	Steps
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.

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

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

SETTING	DESCRIPTION
DhcpThreadNum=x	Specify the thread number for DHCP mode. The minimum is 3, the maximum is 100. The default value is 3.

SETTING	DESCRIPTION
DhcpDelayScan=x	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.
LogReport=x	0 disables logging, 1 enables logging. Vulnerability Scanner sends the results of the scan to the WFBS server. Logs display in the **System Event Logs** screen on the web console.
OsceServer=x	This is the WFBS server's IP address or DNS name.
OsceServerPort=x	This is the web server port on the WFBS server.

2. Launch Vulnerability Scanner.

TO LAUNCH VULNERABILITY SCANNER ON:	STEPS
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.

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.

To Launch Vulnerability Scanner On:	Steps	
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.

   > **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.

   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 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*.

SETTINGS	DESCRIPTION AND INSTRUCTIONS
Product Query	Vulnerability Scanner can check for the presence of security software on the target clients. 1. Select the security software to check. 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. 3. For Norton Antivirus Corporate Edition, you can change the timeout settings by clicking **Settings**.

	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 8and 64.
	
	   For example, type `ThreadNumSchedule=50` if you want Vulnerability Scanner to check 50 client at the same time.
	
	3. Save TMVS.ini.

SETTINGS	DESCRIPTION AND INSTRUCTIONS
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.

SETTINGS	DESCRIPTION AND INSTRUCTIONS
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.
Security Server settings	1. Select **Auto-install Security Agent on unprotected computers** to install the Security Agent to the clients that Vulnerability Scanner will scan. 2. Type the Security Server host name or IPv4/IPv6 address and port number. Security Agents installed by Vulnerability Scanner will report to this server. 3. Configure the administrative credentials to use when logging on to the clients by clicking **Install Account**. In the **Account Information** screen, type a user name and password and click **OK**.

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 Computer**.

   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:

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

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 8/8.1, 10, Server 2012, and Server 2012 R2.

  - 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

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

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

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

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:

http://docs.trendmicro.com/en-us/smb/worry-free-business-security.aspx

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.

- The Messaging Security Agent does not support some Microsoft Exchange Server Enterprise features such as data availability group (DAG).

Procedure

1. Navigate to **Security Settings** > **Add Computer**.

   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 **Manage Client Tree** > **Remove Group/Client**.

    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 **Manage Client Tree** > **Remove Group/Client**.

   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 3-41*.

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

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.

3. On the target client, run SA_Uninstall.exe.

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.

TASK	STEPS
Uninstall the Security Agent	a. Run **Uninstall.bat**. There are several ways to perform this step. • On Windows Vista, 7, 8/8.1, 10, Server 2008/2012/2012 R2, 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.
Unload the Security Agent	a. Run **Stop.bat**. There are several ways to perform this step. • On Windows Vista, 7, 8/8.1, 10, Server 2008/2012/2012 R2, or SBS 2011, navigate to the tool's directory, right-click **Stop.bat**, and select **Run as Administrator**. At the UAC screen, select **Agree**. • On Windows XP/2003, double-click **Stop.bat**. b. Verify that the program ends when the client is stopped.

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**.

3. Locate **Trend Micro Messaging Security Agent** and click **Change**.

4. Follow the on-screen instructions.

Chapter 4

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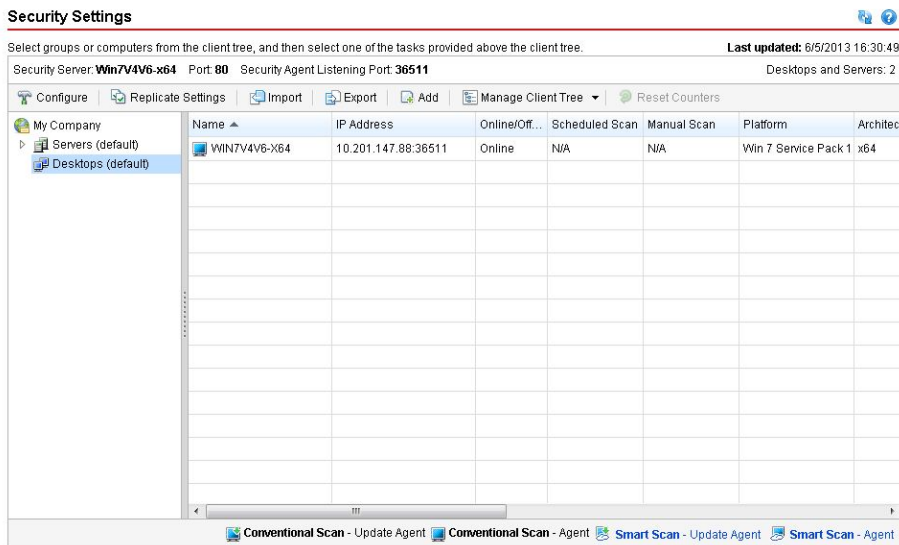
FIGURE 4-1. Security Settings screen showing agents in a group

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.

COLUMN	INFORMATION SHOWN
For Security Agents	
Name	Host name of the client where the agent is installed
IP Address	IP address of the client where the agent is installed
Online/Offline	• **Online**: The agent is connected to the Security Server • **Offline**: The agent is disconnected from the Security Server
Scheduled Scan	Date and time of the last Scheduled Scan
Manual Scan	Date and time of the last Manual Scan
Platform	Operating system of the client where the agent is installed
Architecture	• **x64**: 64-bit operating system • **x86**: 32-bit operating system
Scan Method	• **Smart**: Local and in-the-cloud scans • **Conventional**: Local scans only For details, see *Scan Methods on page 5-3*.
Virus Engine	Virus Scan Engine version

Column	Information Shown
Smart Scan Agent Pattern **Note** This column only displays if the scan method is smart scan.	Smart Scan Agent Pattern version
Smart Scan Service **Note** This column only displays if the scan method is smart scan.	• **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 **Note** This column only displays if the scan method is conventional scan.	Virus Pattern version
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

Column	Information Shown
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
Online/Offline	• **Online**: The agent is connected to the Security Server • **Offline**: The agent is disconnected from the Security Server
Platform	Operating system of the client where the agent is installed
Architecture	• **x64**: 64-bit operating system • **x86**: 32-bit operating system
Exchange Version	Microsoft Exchange server version
Virus Pattern	Virus Pattern version
Virus Engine	Virus Scan Engine version
Version	Version of the agent

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.

Task	Target	Description
Configure	One Security Agent group (desktop or server)	Configure the following basic security settings for all Security Agents belonging to the selected group: • Scan method. See *Configuring Scan Methods on page 5-5*. • Antivirus/Anti-spyware. See *Configuring Real-time Scan for Security Agents on page 5-7*. • Firewall. See *Configuring the Firewall on page 5-10*. • Web Reputation. See *Configuring Web Reputation for Security Agents on page 5-16*. • URL Filtering. See *Configuring URL Filtering on page 5-18*. • Approved/Blocked URLs. See *Approved/Blocked URLs on page 5-19*. • Behavior Monitoring. See *Configuring Behavior Monitoring on page 5-21*. • Device Control. See *Configuring Device Control on page 5-25*. • User Tools (desktop groups only). See *Configuring User Tools on page 5-27*. • Client Privileges. See *Configuring Agent Privileges on page 5-28*. • Quarantine. See *Configuring the Quarantine Directory on page 5-33*.

TASK	TARGET	DESCRIPTION
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 6-8* 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 6-44*. • Web Reputation. See *Configuring Web Reputation for Messaging Security Agents on page 6-48*. • Quarantine. See *Querying Quarantine Directories on page 6-60*, *Maintaining Quarantine Directories on page 6-63*, and *Configuring Quarantine Directories on page 6-64*. • Operations. See *Configuring Notification Settings for Messaging Security Agents on page 6-67*, *Configuring Spam Maintenance on page 6-67*, and *Generating System Debugger Reports on page 6-71*.
Replicate Settings	One Security Agent group (desktop or server)	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*.

Task	Target	Description
Import	One Security Agent group (desktop or server)	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 *Importing and Exporting the Settings of Security Agent Groups on page 4-19*.
Export	One Security Agent group (desktop or server)	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 *Importing and Exporting the Settings of Security Agent Groups on page 4-19*.
Add Group	Security Groups Tree ( )	Add a new Security Agent group (desktop or server group). For details, see *Adding Groups on page 4-10*.
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*.

Task	Target	Description
Remove	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 3-38*.
	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 3-38*.
	One Messaging Security Agent (Advanced only)	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 3-38*.
Move	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*.

Task	Target	Description
Reset Counters	Security Groups Tree (🖥️)	Resets threat counts on all Security Agents to zero. In particular, values under the following columns in the **Agents List** will be reset: • Viruses Detected • Spyware Detected • Spam Detected • URLs Violated For details about these columns, see *Security Groups Tree and Agents List on page 4-2*.

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:

Installing Messaging Security Agents (Advanced only)

See the following topics:

Moving Agents

There are several ways to move agents.

AGENT TO MOVE	DETAILS	HOW TO MOVE AGENTS
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*.

Moving Security Agents Between Groups

Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Select the agents to move.

> ### 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.

> **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 **Manage Client Tree** > **Move Client**.

   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 client, open a command prompt.

    > **Note**
    >
    > You must open the command prompt as administrator.

2. Type `cd` and the path to the Security Agent installation folder. For example: `cd C:\Program Files\Trend Micro\Security Agent`

3. Run Client Mover using the following syntax:

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

TABLE 4-1. Client Mover Parameters

PARAMETER	EXPLANATION
`<executable file name>`	IpXfer.exe
`<server name>`	The name of the destination WFBS server (the server to which the agent will transfer)
`<server listening port>`	The listening port (or trusted port) of the destination Security Server.

PARAMETER	EXPLANATION
`<client listening port>`	The port number used by the Security Agent to communicate with the server

Example:

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

4. 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 **More** > **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 **More** > **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.

SELECTION	SCREEN THAT CONTAINS THE SETTINGS	SETTINGS THAT CAN BE EXPORTED/IMPORTED
Security Groups Tree icon ( )	Security Settings (**Security Settings** > **Configure Settings**)	The following settings for the **Servers (Default)** and **Desktops (Default)** groups: • Scan Method • Firewall • Web Reputation • URL Filtering • Approved/Blocked URLs • Behavior Monitoring • Trusted Program • User Tools (Available only on desktop groups) • Client Privileges • Quarantine • Device Control
	Manual Update (**Updates** > **Manual**)	Components selected in the Manual Update screen
	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**

SELECTION	SCREEN THAT CONTAINS THE SETTINGS	SETTINGS THAT CAN BE EXPORTED/IMPORTED
Desktop group (🖳) or Server group (🖳)	Security Settings (**Security Settings** > **Configure Settings**)	• Antivirus/Anti-spyware Real-time Scan • Firewall • Web Reputation • URL Filtering • Behavior Monitoring • Trusted Program • User Tools (**Available only on desktop groups**) • Client Privileges • Quarantine • Device Control
	Manual Scan screen (**Scans** > **Manual Scan**)	All settings
	Scheduled Scan screen (**Scans** > **Scheduled Scan**)	All settings

Exporting Settings

Procedure

1. Navigate to **Security Settings**.

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

3. Click **More** > **Export**.

    A new screen appears.

4. If you selected the Security Groups Tree, select the settings to export.

5.   Click **More** > **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 **More** > **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 5-1. Summary of Basic Security Settings for Security Agents

OPTION	DESCRIPTION	DEFAULT
Scan Method	Configure whether Smart Scan is enabled or disabled.	Enabled or Disabled is chosen during installation.
Antivirus/Anti-spyware	Configure Real-time Scan, antivirus, and anti-spyware options	Enabled (Real-time Scan)
Firewall	Configure Firewall options	Disabled
Web Reputation	Configure In Office and Out of Office Web Reputation options	In Office: Enabled, Low Out of Office: Enabled, Medium
URL Filtering	URL filtering blocks websites that violate configured policies.	Enabled, Low
Approved/Blocked URLs	Configure the global approved/blocked lists	Disabled
Behavior Monitoring	Configure Behavior Monitoring options	Enabled for Desktop Groups Disabled for Server Groups
Trusted Program	Specify which programs do not need to be monitored for suspicious behavior	N/A
Device Control	Configure Autorun and USB and network access	Disabled

OPTION	DESCRIPTION	DEFAULT
User Tools	Configure Wi-Fi Advisor and Trend Micro Anti-spam Toolbar	Disabled: Wi-Fi Advisor Disabled: Anti-spam Toolbar in supported email clients
Client Privileges	Configure access to settings from the agent console Disable Security Agent upgrade and hot fix deployment	N/A
Quarantine	Specify the Quarantine directory	http://<Security Server name or IP address>

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

BASIS OF COMPARISON	CONVENTIONAL SCAN	SMART SCAN
Scanning behavior	The conventional scan Security Agent performs scanning on the client.	• The smart scan agent performs scanning on the client. • If the Security Agent cannot determine the risk of the file during the scan, the Security Agent verifies the risk by sending a scan query to the Scan Server (for Security Agents connected to the Smart Scan Server) or the Trend Micro Smart Protection Network (for Security Agents disconnected from the Smart Scan Server). **Note** The Scan Server is a service running on the Smart Scan Server. • The Security 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	ActiveUpdate Server	ActiveUpdate 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

CONSIDERATION	DETAILS
Security Server connection	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.

CONSIDERATION	DETAILS
Number of Security Agents to switch	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.
Timing	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 "Update Now" on agents to prevent user-initiated updates and re-enable it after the agents have switched scan methods. **Note** Subsequently, agents will download **smaller, incremental** versions of the Smart Scan Agent Pattern or Virus Pattern as long as they are updated frequently.
IPv6 support	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.

Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure Settings**.

   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 Settings**.

     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

SETTINGS	STATUS
Security Level	Low Inbound and outbound traffic allowed, only network viruses blocked.
Intrusion Detection System	Disabled
Alert Message (send)	Disabled

TABLE 5-5. Default Firewall Exceptions

EXCEPTION NAME	ACTION	DIRECTION	PROTOCOL	PORT
DNS	Allow	Incoming and outgoing	TCP/UDP	53
NetBIOS	Allow	Incoming and outgoing	TCP/UDP	137, 138, 139, 445
HTTPS	Allow	Incoming and outgoing	TCP	443
HTTP	Allow	Incoming and outgoing	TCP	80
Telnet	Allow	Incoming and outgoing	TCP	23
SMTP	Allow	Incoming and outgoing	TCP	25
FTP	Allow	Incoming and outgoing	TCP	21
POP3	Allow	Incoming and outgoing	TCP	110
MSA	Allow	Incoming and outgoing	TCP	16372, 16373
LDAP	Allow	Incoming and outgoing	TCP/UDP	389

TABLE 5-6. Default Firewall Settings According to Location

LOCATION	FIREWALL SETTINGS
In Office	Off
Out of Office	Off

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 Settings**.

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

5. Select **Enable Firewall**.

6. Select from the following:

    •   **Simple Mode**: Enables firewall with default settings.

        For details, see *Firewall 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.

For details, see *Working with Firewall Exceptions on page 5-12*

8. Click **Save**.

Working with Firewall Exceptions

The Firewall exception list contains entries you can configure to allow or block different kinds of network traffic based on client port numbers and IP 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 Settings**.

    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 Settings**.

   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*.
>
> If Web Reputation and Brower Exploit Prevention are both enabled, URLs that are not blocked by Web Reputation are then scanned by Brower Exploit Prevention. Brower Exploit Prevention scans the embedded objects (for example: jar, class, pdf, swf, html, js) in the URL's web pages.

Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure Settings**.

    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**

    •   Browser Exploit Prevention: **Block pages containing malicious script**

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.

Note

> To protect customers, Trend Micro automatically blocks all URLs that contain content considered as illegal in most parts of the world.

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 Settings**.

    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.

6. Click **Save**.

Approved/Blocked URLs

Automatic URL approval and blocking helps you control access to websites and create a safer Internet environment. Identify approved or blocked URLs in the Global Settings.

It is also possible to create customized URL approval and blocking lists for specific groups. When the option **Customize approved/blocked URLs for this group** is selected, the Security Agent uses the group's customized list of approved or blocked URLs to control access to websites.

Configuring Approved/Blocked URLs

Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure Settings**.

    A new screen appears.

4. Click **Approved/Blocked URLs**.

    A new screen appears.

5. Update the following as required.

- • **Customize approved/blocked URLs for this group**: The URLs specified in this list override all other settings.

- • In the **URLs to approve** text box, type the URLs of websites to exclude from Web Reputation and URL Filtering verifications. Separate multiple URLs with a semicolon (;). Click **Add**.

💡 **Tip**

Click **Import from Global Settings** to insert all the entries. You can then customize the URLs for this group.

- • In the **URLs to block** text box, type the URLs of websites to block during URL Filtering. Separate multiple URLs with a semicolon (;). Click **Add**.

💡 **Tip**

Click **Import from Global Settings** to insert all the entries. You can then customize the URLs for this group.

---

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. When Behavior Monitoring is enabled, users create exceptions to approve or block specific programs. 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 Settings**.

4. Click **Behavior Monitoring**.

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 Malware Behavior Blocking for known and potential threats**:
      Malware behavior blocking is accomplished using a set of internal rules
      defined in **pattern files**. These rules identify known and suspicious threat
      behavior that is common amongst malware. Examples of suspicious behavior
      includes sudden and unexplainable new running services, changes to the
      firewall, or system file modifications.

        - **Known threats**: Blocks behavior associated with known threats

        - **Known and potential threats**: Blocks behavior associated with known
          threats and takes action on behavior that is potentially malicious

    - **Prompt users before executing newly encountered programs
      downloaded through HTTP (server platforms excluded)**: Behavior
      Monitoring works in conjunction with Web Reputation to verify the
      prevalence of files downloaded through HTTP channels or email applications.
      After detecting a "newly encountered" file, administrators can choose to
      prompt users before executing the file. Trend Micro classifies a program as

newly encountered based on the number of file detections or historical age of the file as determined by the Smart Protection Network.

> **Note**
>
> For HTTP channels, executable (.exe) files are scanned. For email applications (only Outlook and Windows Live Mail), executable (.exe) files in non-password protected archived (zip/rar) files are scanned.

• **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.

• Under **Ransomware Protection**, update the following:

> **Note**
>
> Ransomware Protection prevents the unauthorized modification or encryption of files on computers by "ransomware" threats. Ransomware is a type of malware which restricts access to files and demands payment to restore the affected files.

- **Enable document protection against unauthorized encryption or modification**: Protects documents from unauthorized changes.

    - **Auto backup files changed by suspicious programs**: Automatically backs up files modified by suspicious programs if document protection is enabled.

- **Enable blocking of processes commonly associated with ransomware**: Protects endpoints from ransomware attacks by blocking processes commonly associated with hijacking atempts.

> **Note**
>
> To reduce the chance of WFBS detecting a safe process as malicious, ensure that the computer has Internet access to perform additional verification processes using Trend Micro servers.

- **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.

ENVIRONMENT VARIABLE	POINTS TO THE...
$windir$	Windows folder
$rootdir$	root folder

ENVIRONMENT VARIABLE	POINTS TO THE...
$tempdir$	Windows temporary folder
$programdir$	Program Files folder

- • **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 Settings**.

    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. Specifically, Device Control restricts access to all kinds of storage devices that connect through a USB interface, except smartphones and digital cameras.

Configuring Device Control

Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure Policy**.

    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 5-7. Device Control Permissions

PERMISSIONS	FILES ON THE DEVICE	INCOMING FILES
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 Prohibited operations: Execute	Permitted operations: Save, Move, Copy
Read and execute	Permitted operations: Copy, Open, Execute Prohibited operations: Save, Move, Delete	Prohibited operations: Save, Move, Copy
Read	Permitted operations: Copy, Open Prohibited operations: Save, Move, Delete, Execute	Prohibited operations: Save, Move, Copy
No access	Prohibited operations: All operations The device and the files it contains are visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy

- **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

- **Anti-Spam Toolbar**: Filters spam in Microsoft Outlook, gives statistics, and allows you to change certain settings.

- **HouseCall**: 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.

- **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.

- **Client Mover**: Use this tool to transfer clients from one server to another. The servers must be of the same language version and type.

- **Client-Server Communication Tool**: Use this tool to troubleshoot client-server communication.

Configuring User Tools

Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure Settings**.

   A new screen appears.

4. Click **User Tools**.

    A new screen appears.

5. Update the following as required:

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

    • **Anti-Spam Toolbar**: Filters spam in Microsoft Outlook.

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 Agent Privileges

Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure Settings**.

4. Click **Agent Privileges**.

5. Update the following as required:

SECTION	PRIVILEGES
Antivirus/Anti-spyware	• Manual Scan settings • Scheduled Scan settings • Real-time Scan settings • Skip Scheduled Scan
Firewall	Firewall Settings
Web Reputation - Continue Browsing	Will show a link that allows users to continue browsing a particular malicious URL until the computer is restarted. Warnings will still show on other malicious URLs.
URL Filtering - Continue Browsing	Will show a link that allows users to continue browsing a particular restricted URL until the computer is restarted. Warnings will still show on other restricted URLs.
Behavior Monitoring	Allow users to modify Behavior Monitoring settings.
Trusted Program	Allow users to modify the Trusted Program list.
Proxy Settings	Allow users to configure proxy settings. **Note** Disabling this feature will reset the proxy settings to their default.

SECTION	PRIVILEGES
Update Privileges	• Allow users to perform manual updates • Use Trend Micro ActiveUpdate as a secondary update source • Disable hot fix deployment --- **Note** Deploying hot fixes, patches, security/critical patches, and service packs to a large number of agents simultaneously can significantly increase network traffic. Consider enabling this option on several groups so you can stagger the deployment. Enabling this option also disables automatic **build upgrades** on agents (for example, from the Beta build to the release build of the current product version) but NOT automatic **version upgrades** (for example, from version 7.x to the current version). To disable automatic version upgrades, run the Security Server installation package and choose the option for delaying upgrades.
Client Security	Prevent users or other processes from modifying Trend Micro program files, registries and processes.

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

QUARANTINE DIRECTORY	ACCEPTED FORMAT	EXAMPLE	NOTES
Default directory on the Security Server	URL	http:// <server host name or IP>	If you keep the default directory, configure maintenance settings for the directory, such as the size of the quarantine folder, in **Preferences** > **Global Settings** > **System tab** > **Quarantine Maintenance** section.
	UNC path	\\<server host name or IP>\ ofcscan\Virus	
Another directory on the Security Server	UNC path	\\<server host name or IP>\ D$\Quarantined Files	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** > **Global Settings** > **System tab** > **Quarantine Maintenance** section to allow maintenance settings to take effect.
A directory on another Security Server computer (if you have other Security Servers on the network)	URL	http:// <server2 host name or IP>	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 "Unable to send the quarantined file to the designated quarantine folder".
	UNC path	\\<server2 host name or IP>\ ofcscan\Virus	
Another computer on the network	UNC path	\\<computer_ name> \temp	If you use UNC path, ensure that the quarantine directory folder is shared to the group "Everyone" and that you assign read and write permission to this group.

QUARANTINE DIRECTORY	ACCEPTED FORMAT	EXAMPLE	NOTES
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.

Configuring the Quarantine Directory

Procedure

1. Navigate to **Security Settings**.

2. Select a desktop or server group.

3. Click **Configure Settings**.

    A new screen appears.

4. Click **Quarantine**.

    A new screen appears.

5. Configure the quarantine directory. For details, see *Quarantine Directory on page 5-30*.

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 Messaging Security Agent does not support some Microsoft Exchange Server Enterprise features such as data availability group (DAG).

- 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

SCAN OPTION	REAL-TIME SCAN	MANUAL AND SCHEDULED SCAN
Anti-spam		
Spam	Quarantine message to user's spam folder (default, if the Outlook Junk Email or End User Quarantine installed)	Not applicable
Phish	Delete entire message	Not applicable
Content filtering		
Filter messages that match any condition defined	Quarantine entire message	Replace
Filter messages that match all conditions defined	Quarantine entire message	Not applicable
Monitor the message content of particular email accounts	Quarantine entire message	Replace
Create an exception for particular email accounts	Pass	Pass
Attachment blocking		
Action	Replace attachment with text/file	Replace attachment with text/file
Other		

Scan Option	Real-time Scan	Manual and Scheduled Scan
Encrypted and Password protected files	Pass (When you configure the action to Pass, encrypted files and files that are protected by passwords are passed and the event is not logged)	Pass (When you configure the action to Pass, encrypted files and files that are protected by passwords are passed and the event is not logged)
Excluded files (Files over specified scanning restrictions)	Pass (When you configure the action to Pass, files or message body over the specified scanning restrictions are passed and the event is not logged)	Pass (When you configure the action to Pass, files or message body over the specified scanning restrictions are passed and the event is not logged)

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 Settings**.

   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 7-16*.

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 Settings**.

   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**.

7. Go to: http://ers.trendmicro.com/ to view reports.

> **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 Settings**.

   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 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 1-24*.

    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.

> **Note**
>
> For details about actions, see *Scan Targets and Actions for Messaging Security Agents on page 7-16*.

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 6-67*.

- **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

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

PATTERN	MATCHED SAMPLES	UNMATCHED SAMPLES
.example.com.	john@ms1.example.com.us john@ms1.rd.example.com.us mary@ms1.example.com.us	john@example.com john@ms1.example.com john@trend.example.us
..*.example.com *****.example.com	The same as "*.example.com"	
example.com example.com example.*.com @*.example.com	Invalid patterns	

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.

> **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 6-9*.

The content filter provides a means for the Administrator to evaluate and control the delivery of email on the basis of the message text itself. It can be used to monitor inbound and outbound messages to check for the existence of harassing, offensive, or

otherwise objectionable message content. The content filter also provides a synonym checking feature which allows you to extend the reach of your policies. You can, for example, create rules to check for:

• Sexually harassing language

• Racist language

• Spam embedded in the body of an email message

Note

> By default, content filtering is not enabled.

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:

TASK	STEPS
Enable/Disable Content Filtering	Select or clear **Enable real-time content filtering** on top of the screen.
Add a rule	Click **Add**. A new screen opens where you can choose the type of rule to add. For details, see *Types of Content Filtering Rules on page 6-19*.

Task	Steps
Modify a rule	a. Click the rule name. A new screen opens. b. The options available in the screen depend on the type of rule. To determine the type of rule, check the breadcrumb on top of the screen and note the second item in the breadcrumb. For example: Content Filtering > **Match Any Condition Rule** > Edit Rule For details about rule settings that you can modify, see any of the following topics: • *Adding a Content Filtering Rule for Any Matching Condition on page 6-23* • *Adding a Content Filtering Rule for All Matching Conditions on page 6-20* **Note** This rule type is not available for Manual and Scheduled Content Filtering Scans. • *Adding a Content Filtering Monitoring Rule on page 6-25* • *Creating Exceptions to Content Filtering Rules on page 6-28*

Task	Steps
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. **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. 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.

Task	Steps
Remove rules	When you delete a rule, the Messaging Security Agent updates the order of the other rules to reflect the change. **Note** Deleting a rule is irreversible, consider disabling a rule instead of deleting. a. Select a rule. b. Click **Remove**.

3. Click **Save**.

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 6-23*.

• **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 6-20*.

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 6-25*.

- **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 6-28*.

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 Settings**.

   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 7-16*):

    • 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

    • Pass entire message

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 Settings** > **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

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

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 7-16*):

    •   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 Settings** > **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 7-16*):

    • 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 Settings** > **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

SUPPORTED	NOT SUPPORTED
2007 x64	2003 x86/x64
2010 x64	2007 x86

SUPPORTED	NOT SUPPORTED
	2010 x86

Preparatory Work

Before monitoring sensitive data for potential loss, determine the following:

- Which data needs protection from unauthorized users

- Where the data resides

- Where and how the data is transmitted

- Which users are authorized to access or transmit this information

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

The 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 6-30*.

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 Settings** > **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 6-38*). 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 (🔍) 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:

TASK	STEPS
Enable/Disable Data Loss Prevention	Select or clear **Enable real-time Data Loss Prevention** on top of the screen.
Add a rule	Click **Add**. A new screen opens where you can choose the type of rule to add. For details, see *Adding Data Loss Prevention Rules on page 6-39*.
Modify a rule	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 6-39*.

TASK	STEPS

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. ---

Task	Steps
	To import rules:
	a. 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.
	b. Click **Import**.
	A new window opens.
	c. Click **Browse** to locate the file to import, and then click **Import**.
	Data Loss Prevention imports the rules in the file and appends them to the end of the current rules list.
	Tip If you already have more than 10 rules, the imported rules will not be visible on the first page. Use the page-navigation icons at the top or bottom of the rules list to display the last page of the list. The newly imported rules should be there.

Task	Steps
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. 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. **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. 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.

Task	Steps
Remove rules	When you delete a rule, the Messaging Security Agent updates the order of the other rules to reflect the change. **Note** Deleting a rule is irreversible, consider disabling a rule instead of deleting. a. Select a rule. b. Click **Remove**.

TASK	STEPS
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.

Task	Steps
Add email accounts to the Approved Senders List	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. a. Click the plus (+) icon to expand the **Approved Senders** section. b. Place your cursor in the **Add** field and type the full email address, using the following pattern: `example@example.com` c. Click **Add**. The address appears in the list shown below the **Add** field. d. Click **Save** to complete the process. **Note** 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.

Import email accounts to the Approved Senders List	You can import a list of email addresses from a plain-text file formatted with one email account per line, such as:
	
	 `admin@example.com`
	
	 `ceo@example.com`
	
	 `president@example.com`
	
	 a. Click the plus (+) icon to expand the **Approved Senders** section.
	
	 b. Click **Import**.
	
	 A new window opens.
	
	 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.

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

RULE NAME	EXAMPLE	REGULAR EXPRESSION
Visa Card account number	4111-1111-1111-1111	.REG. \b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
MasterCard account number	5111-1111-1111-1111	.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
American Express account number	3111-111111-11111	.REG. \b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Diners Club/ Carte Blanche account number	3111-111111-1111	.REG. [^\d-]((36\d{2}|38\d{2}|30[0-5]\d)-?\d{6}-?\d{4})[^\d-]
IBAN	BE68 5390 0754 7034, FR14 2004 1010 0505 0001 3M02 606, DK50 0040 0440 1162 43	.REG. [^\w]((([A-Z]{2}\d{2}[-|\s]?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}[-|\s]){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}[-|\s]){2}[A-Za-z0-9]{3,4}))[^\w]
Swift BIC	BANK US 99	.REG. [^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-]
ISO date	2004/01/23, 04/01/23, 2004-01-23, 04-01-23	.REG. [^\d\V-]([1-2]\d{3}[-\V][0-1]?\d[-\V][0-3]?\d|\d{2}[-\V][0-1]?\d[-\V][0-3]?\d)[^\d\V-]

> **Note**
>
> A zip file containing more DLP rules can be downloaded from the web console. Navigate to **Security Settings** > **{Messaging Security Agent}** > **Configure Settings** > **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 Settings**.

    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-10* 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-10* 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 7-16*):

• 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

• 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 Settings** > **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 7-16*):

    *   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:

    * **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 Settings**.

    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 7-16*):

   • 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**.

Mobile Security

Mobile security settings prevent unauthorized devices from accessing and downloading information from the Microsoft Exchange Server. Administrators identify which devices are allowed to access the Microsoft Exchange Server, and then identify whether the users of those devices can download or update their email, calendar, contacts, or tasks.

Administrators can also apply security policies to devices. These policies control password length and complexity, whether devices should be locked after a period of inactivity, whether devices are required to use encryption, and whether device data should be wiped following a series of unsuccessful sign-in attempts.

Mobile Security Support

TABLE 6-5. Mobile Device Support

OS	IIS VERSION	DEVICE DATA PROTECTION POLICIES		ACCESS CONTROL		
		EXCHANGE 2007 (OR ABOVE) 64-BIT	EXCHANGE 2003 32-BIT	EXCHANGE 2010 (AND ABOVE) 64-BIT	EXCHANGE 2007 64-BIT	EXCHANGE 2003 32-BIT
• Windows 2008 (64-bit) • SBS 2008 (64-bit)	7 +	Yes	Incompatible	Yes	No	Incompatible
Windows 2003 (64-bit)	6.0	Yes	Incompatible	No	No	Incompatible

OS	IIS VERSION	DEVICE DATA PROTECTION POLICIES		ACCESS CONTROL		
		EXCHANGE 2007 (OR ABOVE) 64-BIT	EXCHANGE 2003 32-BIT	EXCHANGE 2010 (AND ABOVE) 64-BIT	EXCHANGE 2007 64-BIT	EXCHANGE 2003 32-BIT
• Windows 2003 (32-bit) • SBS 2003 (32-bit)	6.0	Incompatible	No	Incompatible	Incompatible	No

TABLE 6-6. Mobile Device OS Support

MOBILE OS	OS VERSION
iOS	3.0 - 6.1 (4.3 - 7.0)
Android	2.2 - 4.2
WM/WP (Windows)	7.0 - 8.0
BB (BlackBerry)	7.0 - 10.1

Configuring Device Access Control

Procedure

1. Navigate to **Security Settings**.

2. Select a Messaging Security Agent.

3. Click **Configure Settings**.

A new screen appears.

4. Click **Mobile Security** > **Device Access Control**.

    A new screen appears.

5. Select **Enable Device Access Control**.

6. Click **Add**.

7. Type a policy name and a meaningful description for the policy.

8. Select which devices to allow/block access to the Microsoft Exchange Server by identifying the device owner(s):

    • **Anyone**

    • **Specify device owners**

9. If **Specify device owners** is selected:

    a. Type a device owner's name and click **Search** to find the device owner in the Microsoft Exchange Server's Global Address List.

    b. Select the device owner and click **Add**.

10. If it is known, select the device's operating system from the **Type** drop-down list.

11. If it is known, select **Specify version number range** and identify which versions of that operating system are allowed.

12. Specify whether the Messaging Security Agent should allow or block access to the device owner's mail, calendar, contacts, or tasks.

13. Click **Save**.

Cancelling a Pending Device Wipe

Procedure

1. Navigate to **Security Settings**.

2. Select a Messaging Security Agent.

3. Click **Configure Settings**.

   A new screen appears.

4. Click **Mobile Security** > **Device Wipe**.

   A new screen appears.

5. Identify the device in the device wipe table and click **Cancel Wipe**.

6. Click **OK**.

Manually Wiping Devices

Procedure

1. Navigate to **Security Settings**.

2. Select a Messaging Security Agent.

3. Click **Configure Settings**.

   A new screen appears.

4. Click **Mobile Security** > **Device Wipe**.

   A new screen appears.

5. Click **Select Devices**.

   A new screen appears.

6. Type a device owner's name and click **Search** to find their device.

7. If the device is available to wipe, select the device and click **Wipe**.

> **Note**
>
> It is not possible to select a device if the device status after a search is **Wipe successful** or **Wipe pending**.

Configuring Security Policies

WFBS uses the Microsoft Exchange default policy as the default policy. The default policy appears in the Security Policy list.

WFBS does not maintain non-default policies added using the Microsoft Exchange management console or the Exchange Cmdlet.

Trend Micro recommends administrators manage security policies from WFBS management console or Microsoft Exchange.

Procedure

1. Navigate to **Security Settings**.

2. Select a Messaging Security Agent.

3. Click **Configure Settings**.

   A new screen appears.

4. Click **Mobile Security** > **Security Policies**.

   A new screen appears.

5. Click **Add**.

6. Type a policy name and a meaningful description for the policy.

7. Type a device owner's name and click **Search** to find the device owner in the Microsoft Exchange Server's Global Address List.

8. Select the device owner and click **Add**.

9. Select the security criteria to apply to the device:

- • **Minimum password length**: For guidelines on mobile device passwords, see *Password Complexity Requirements on page 6-55*.

- • **Minimum number of required character sets**: For guidelines on mobile device passwords, see *Password Complexity Requirements on page 6-55*.

- • **Lock device after inactivity**

- • **Require encryption on device**: The mobile device must support encryption.

- • **Wipe device after unsuccessful sign-in**

10. Click **Save**.

Password Complexity Requirements

The password complexity requirements differ for different device types and operating systems.

The following tables list the behavior of each complexity "Option" for the devices tested at the time of the WFBS 9.0 SP1 release.

> **Note**
>
> The functionality of password complexity is dependent on the device type and operating system version. If the specified password does not comply with the complexity requirements, most devices provide users with a message that indicates what the specific requirements are for the device.

TABLE 6-7. Android Devices

COMPLEXITY LEVEL	COMPLEXITY REQUIREMENTS	
	ANDROID 4	ANDROID 2
Option 1	A combination of the following types of characters: • At least one uppercase (A-Z) or lowercase (a-z) character • At least one number (0-9) or special character (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	Alphanumeric
Option 2	A combination of the following types of characters: • At least one uppercase (A-Z) or lowercase (a-z) character • At least two numbers (0-9) or special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	A combination of the following types of characters: • Alphanumeric • At least two numbers (0-9) or special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 3	A combination of the following types of characters: • At least one uppercase (A-Z) or lowercase (a-z) character • At least three numbers (0-9) or special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	A combination of the following types of characters: • Alphanumeric • At least three numbers (0-9) or special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 4	A combination of the following types of characters: • At least one uppercase (A-Z) or lowercase (a-z) character • At least four numbers (0-9) or special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	A combination of the following types of characters: • Alphanumeric • At least four numbers (0-9) or special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

TABLE 6-8. iOS Devices

COMPLEXITY LEVEL	COMPLEXITY REQUIREMENTS
Option 1	A combination of the following types of characters: • Alphanumeric • At least one special character (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 2	A combination of the following types of characters: • Alphanumeric • At least two special characters (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 3	A combination of the following types of characters: • Alphanumeric • At least three special characters (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 4	A combination of the following types of characters: • Alphanumeric • At least four special characters (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

TABLE 6-9. Windows Phone Devices

COMPLEXITY LEVEL	COMPLEXITY REQUIREMENTS	
	WINDOWS PHONE 8	WINDOWS PHONE 7
Option 1	At least one of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	A combination of at least two of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Complexity Level	Complexity Requirements	
	Windows Phone 8	Windows Phone 7
Option 2	A combination of at least two of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	A combination of at least two of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 3	A combination of at least three of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	A combination of at least three of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 4	A combination of all of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)	A combination of all of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

TABLE 6-10. BlackBerry Devices

Complexity Level	Complexity Requirements
Option 1	At least one uppercase (A-Z) or lowercase (a-z) character

COMPLEXITY LEVEL	COMPLEXITY REQUIREMENTS
Option 2	A combination of at least two of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 3	A combination of at least three of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Option 4	A combination of all of the following types of characters: • Uppercase characters (A-Z) • Lowercase characters (a-z) • Numeric characters (0-9) • Special characters (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

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 and Spyware (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 Settings**.

    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 6-61*.

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 ().

> 📝 **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 Settings**.

   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 Settings**.

   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 Settings**.

    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 Settings**.

    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 6-69*.

    > **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 .

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 users 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 Settings**.

    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)** on Exchange Server 2003, 2007, or 2010

    •   **Store Level Scan** on Exchange Server 2013

    •   **Simple Mail Transfer Protocol (SMTP)** on Exchange Server 2003

    •   **Transport Service** on Exchange Server 2007, 2010, or 2013

    •   **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 Settings**.

      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.

INSTRUCTIONS AND NOTES	RECOMMENDED 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** 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.	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 layer 1: Scans compressed files that are 1 compression layer deep. Default is "off" for the default server group and "on" for the default desktop group.
	Exclusions • Do not scan the directories where Trend Micro products are installed
	Advanced Settings • Modify Spyware/Grayware Approved List (for Anti-spyware only)

INSTRUCTIONS AND NOTES	RECOMMENDED SCAN SETTINGS
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 7-16*. • **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 6-44*.	• 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.

INSTRUCTIONS AND NOTES	RECOMMENDED 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.	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 layer 2: Scans compressed files that are 2 compression layers deep.
	Exclusions • Do not scan the directories where Trend Micro products are installed
	Advanced Settings • Modify Spyware/Grayware Approved List (for Anti-spyware only)

INSTRUCTIONS AND NOTES	RECOMMENDED SCAN SETTINGS
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 7-16*. • **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 6-44*.	• 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

Select a method:

- **All scannable files**: includes all scannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions.

  > **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 uses "true file type" identification**: 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.

Select a 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**

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

- Exclude file extensions

  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 TYPE	OPTION
Real-time Scan	**Scan POP3 messages**: By default, Mail Scan can only scan new messages sent through port 110 in the Inbox and Junk Mail folders. It does not support secure POP3 (SSL-POP3). • Outlook Express™ 6.0 with Service Pack 2 (on Windows XP only) • Windows Mail™ (on Microsoft Vista only) • Microsoft Outlook 2000, 2002 (XP), 2003, 2007, 2010, or 2013 • Mozilla Thunderbird 1.5 or higher Mail Scan cannot detect security risks in IMAP messages. Use the Messaging Security Agent (Advanced only) to detect security risks and spam in IMAP messages.
Real-time Scan, Manual Scan	**Scan mapped drives and shared folders on the network**: Select to scan directories physically located on other computers, but mapped to the local computer.
Real-time Scan	**Scan floppy disks during system shutdown**
Real-time Scan	**Enable IntelliTrap**: IntelliTrap detects malicious code, such as bots, in compressed files. See *IntelliTrap on page D-2*.

Scan Type	Option
Real-time Scan	**Quarantine malware variants detected in memory**: If Real-time Scan and Behavior Monitoring are enabled and this option is selected, running process memory is scanned for packed malware. Any packed malware that Behavior Monitoring detects is quarantined.
Real-time Scan, Manual Scan, Scheduled Scan	**Scan compressed files up to layer __**: A compressed file has one layer for each time it has been compressed. If an infected file has been compressed to several layers, it must be scanned through the specified number of layer to detect the infection. Scanning through multiple layers, however, requires more time and resources.
Real-time Scan, Manual Scan, Scheduled Scan	**Modify Spyware/Grayware Approved List**: This setting cannot be configured from the agent console.
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
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.

Action Tab

The following are the actions that Security Agents can perform against viruses/malware:

TABLE 7-1. Virus/Malware Scan Actions

ACTION	DESCRIPTION
Delete	Deletes the infected file.
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.

ACTION	DESCRIPTION
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*.
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

ACTION	DESCRIPTION
Clean	Terminates processes or deletes registries, files, cookies, and shortcuts.
Pass	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 "Deny Access". The Security Agent will not perform any action if the detected spyware/grayware is included in the approved list.
Deny Access	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 "Pass".

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 7-3. Trend Micro Recommended Scan Actions Against Viruses and Malware

VIRUS/MALWARE TYPE	REAL-TIME SCAN		MANUAL SCAN/SCHEDULED SCAN	
	FIRST ACTION	SECOND ACTION	FIRST ACTION	SECOND ACTION
Joke program	Quarantine	Delete	Quarantine	Delete
Trojan horse program/Worms	Quarantine	Delete	Quarantine	Delete
Packer	Quarantine	N/A	Quarantine	N/A
Probable virus/ malware	Quarantine	N/A	Pass or user-configured action	N/A
Virus	Clean	Quarantine	Clean	Quarantine
Test virus	Deny Access	N/A	N/A	N/A
Other malware	Clean	Quarantine	Clean	Quarantine

Notes and Reminders:

• For probable virus/malware, the default action is "Quarantine" during Real-time Scan and "Pass" during Manual Scan and Scheduled Scan. If these are not your preferred actions, you can change them to Delete or Rename.

• Some files are uncleanable. For details, see *Uncleanable Files on page D-26*.

• ActiveAction is not available for spyware/grayware scan.

• The default values for these settings can change, when new pattern files become available.

Advanced Settings

SCAN TYPE	OPTION
Real-time Scan, Scheduled Scan	**Display an alert message on the desktop or server when a virus/spyware is detected**

SCAN TYPE	OPTION
Real-time Scan, Scheduled Scan	**Display an alert message on the desktop or server when a probable virus/spyware is detected**
Manual Scan, Real-time Scan, Scheduled Scan	**Run cleanup when probable virus/malware is detected**: Only available if you choose ActiveAction and customized the action for probable virus/malware.

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 1-21*.

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.

FILE SIZE (NOT COMPRESSED)	FILE SIZE (NOT COMPRESSED)	RESULT
500 KB	10 KB (ratio is 50:1)	Scanned
1000 KB	10 KB (ratio is 100:1)	Scanned
1001 KB	10 KB (ratio exceeds 100:1)	Not scanned *
2000 KB	10 KB (ratio is 200:1)	Not scanned *

* The Messaging Security Agent takes the action you configure for excluded files.

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

ACTION	DESCRIPTION
Clean	Removes malicious code from infected message bodies and attachments. The remaining email message text, any uninfected files, and the cleaned files are delivered to the intended recipients. Trend Micro recommends you use the default scan action clean for virus/malware.

Under some conditions, the Messaging Security Agent cannot clean a file.

During a Manual Scan or Scheduled Scan, the Messaging Security Agent updates the Information Store and replaces the file with the cleaned one. |

Action	Description
Replace with text/ file	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).
Quarantine entire message	(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.
Quarantine message part	(Real-time Scan only) Quarantines only the infected or filtered content to the quarantine directory and the recipient receives the message without this content.
Delete entire message	(Real-time Scan only) Deletes the entire email message. The original recipient will not receive the message.
Pass	Records virus infection of malicious files in the Virus logs, but takes no action. Excluded, encrypted, or password-protected files are delivered to the recipient without updating the logs.
	For Content Filtering, delivers the message as-is.
Archive	Moves the message to the archive directory and delivers the message to the original recipient.
Quarantine message to server-side spam folder	Sends the entire message to the Security Server for quarantine.
Quarantine message to user's spam folder	Sends the entire message to the user's spam folder for quarantine. The folder is located on the server-side of the Information Store.
Tag and deliver	Adds a tag to the header information of the email message that identifies it as spam and then delivers it to the intended recipient.

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

VIRUS/MALWARE TYPE	REAL-TIME SCAN		MANUAL SCAN/SCHEDULED SCAN	
	FIRST ACTION	**SECOND ACTION**	**FIRST ACTION**	**SECOND ACTION**
Virus	Clean	Delete entire message	Clean	Replace with text/file
Trojan horse program/Worms	Replace with text/file	N/A	Replace with text/file	N/A
Packer	Quarantine message part	N/A	Quarantine message part	N/A
Other malicious code	Clean	Delete entire message	Clean	Replace with text/file
Additional threats	Quarantine message part	N/A	Replace with text/file	N/A
Mass-mailing behavior	Delete entire message	N/A	Replace with text/file	N/A

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.

Advanced Settings (Scan Actions)

SETTINGS	DETAILS

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

SETTINGS	DETAILS
Unscannable Message Parts	Set the action and notification condition for encrypted and/or password-protected files. For the action, select from Replace with text/file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part.
Excluded Message Parts	Set the action and notification condition for parts of messages that have been excluded. For the action, select from Replace with text/file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part.
Backup Setting	The location to save the backup of infected files before the agent cleaned them.
Replacement Settings	Configure the text and file for replacement text. If the action is **replace with text/file**, WFBS will replace the threat with this text string and file.

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

UPDATE SEQUENCE	DESCRIPTION	RECOMMENDATION
1. ActiveUpdate Server or custom update source 2. Security Server 3. Agents	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).	Use this method if there are no low-bandwidth sections between the Security Server and agents.

Update Sequence	Description	Recommendation
1. ActiveUpdate Server or custom update source 2. Security Server 3. Update Agents, Messaging Security Agents, Security Agents without Update Agents 4. All other Security Agents	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 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.	If there are low-bandwidth sections between the Security Server and Security Agents, use this method to balance the traffic load on the network.
1. ActiveUpdate Server 2. Security Agents	Security Agents that cannot update from any source update directly from the ActiveUpdate server. --- 📝 **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.

Updatable Components

Worry-Free Business Security makes use of components to keep agents protected from the latest threats. Keep these components up-to-date by running manual or scheduled updates.

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. Worry-Free Business Security 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:

TABLE 8-2. Messaging Components (Advanced only)

COMPONENT	DISTRIBUTED TO	DESCRIPTION
Messaging Security Agent Anti-spam Pattern	Messaging Security Agents	The Anti-spam Pattern identifies the latest spam in email messages and email attachments.
Messaging Security Agent Anti-spam Engine 32/64-bit	Messaging Security Agents	The Anti-spam Engine detects spam in email messages and email attachments.
Messaging Security Agent Scan Engine 32/64-bit	Messaging Security Agents	The Scan Engine detects Internet worms, mass-mailers, Trojans, phishing sites, spyware, network exploits and viruses in email messages and email attachments.
Messaging Security Agent URL Filtering Engine 32/64-bit	Messaging Security Agents	The URL Filtering Engine facilitates communication between Worry-Free Business Security and the Trend Micro URL Filtering Service. The URL Filtering Service is a system that rates URLs and provides rating information to Worry-Free Business Security.

TABLE 8-3. Antivirus and Smart Scan

COMPONENT	DISTRIBUTED TO	DESCRIPTION
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 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

Component	Distributed To	Description
Smart Scan Pattern	Not distributed to Security Agents. This pattern stays in theSecurity Server and is used when responding to scan queries received from Security Agents.	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 **Smart Scan Pattern** contains majority of the pattern definitions. The **Smart Scan Agent Pattern** contains all the other pattern definitions not found on the Smart Scan Pattern.
Smart Scan Agent Pattern	Security Agents using smart scan	The Security Agent scans for security threats using the **Smart Scan Agent Pattern**. Security Agents that cannot determine the risk of the file during the scan verify 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 **Smart Scan Pattern**. The Security Agent "caches" the scan query result provided by the Scan Server to improve the scan performance.
Virus Pattern	Security Agents using conventional scan	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.
IntelliTrap Pattern	Security Agents	The IntelliTrap Pattern detects real-time compression files packed as executable files. For details, see *IntelliTrap on page D-2*.
IntelliTrap Exception Pattern	Security Agents	The IntelliTrap Exception Pattern contains a list of "approved" compression files.

Component	Distributed To	Description
Damage Cleanup Engine 32/64-bit	Security Agents	The Damage Cleanup Engine scans for and removes Trojans and Trojan processes.
Damage Cleanup Template	Security Agents	The Damage Cleanup Template is used by the Damage Cleanup Engine to identify Trojan files and processes so the engine can eliminate them.
Memory Inspection Pattern	Security Agents	This technology provides enhanced virus scanning for polymorphic and mutation viruses, and augments virus-pattern-based scans by emulating file execution. The results are then analyzed in a controlled environment for evidence of malicious intent with little impact on system performance.

TABLE 8-4. Anti-spyware

Component	Distributed To	Description
Spyware/Grayware Scan Engine v.6 32/64-bit	Security Agents	The Spyware Scan Engine scans for and performs the appropriate scan action on spyware/grayware.
Spyware/Grayware Pattern v.6	Security Agents	The Spyware Pattern identifies spyware/grayware in files and programs, modules in memory, Windows registry and URL shortcuts.
Spyware/Grayware Pattern	Security Agents	

TABLE 8-5. Network Virus

Component	Distributed To	Description
Firewall Pattern	Security Agents	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.

TABLE 8-6. Behavior Monitoring and Device Control

COMPONENT	DISTRIBUTED TO	DESCRIPTION
Behavior Monitoring Detection Pattern 32/64-bit	Security Agents	This pattern contains the rules for detecting suspicious threat behavior.
Behavior Monitoring Core Driver 32/64-bit	Security Agents	This kernel mode driver monitors system events and passes them to the Behavior Monitoring Core Service for policy enforcement.
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.
Damage Recovery Engine	Security Agents	The Damage Recovery Engine receives system events and backup files before suspicious threats can modify files and perform other malicious behavior. This engine also restores the affected files after it receives a file recovery request.
Damage Recovery Pattern	Security Agents	The Damage Recovery Pattern contains policies that are used for monitoring suspicious threat behavior.
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.

Component	Distributed To	Description
Policy Enforcement Pattern	Security Agents	The Behavior Monitoring Core Service checks system events against the policies in this pattern.
Memory Scan Trigger Pattern (32/64-bit)	Security Agents	The Memory Scan Trigger service executes other scan engines when it detects the process in memory is unpacked.

TABLE 8-7. Outbreak Defense

Component	Distributed To	Description
Vulnerability Assessment Pattern 32/64-bit	Security Agents	A file that includes the database for all vulnerabilities. The Vulnerability Assessment Pattern provides instructions for the scan engine to scan for known vulnerabilities.

TABLE 8-8. Browser Exploits

Component	Distributed To	Description
Browser Exploit Prevention Pattern	Security Agents	This pattern identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser.
Script Analyzer Pattern	Security Agents	This pattern analyzes script in web pages and identifies malicious script.

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:

- *Critical Patch on page D-2*

- *Hot Fix on page D-2*

- *Patch on page D-9*

- *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:

- 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.
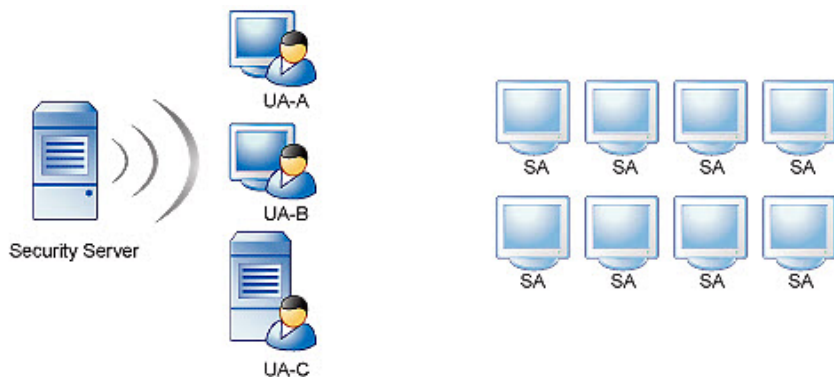
Update Agents

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.

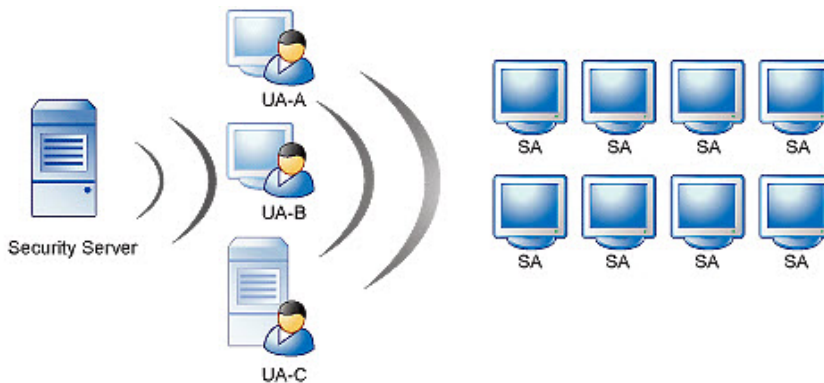The Update Agent update process can be described as follows:

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.
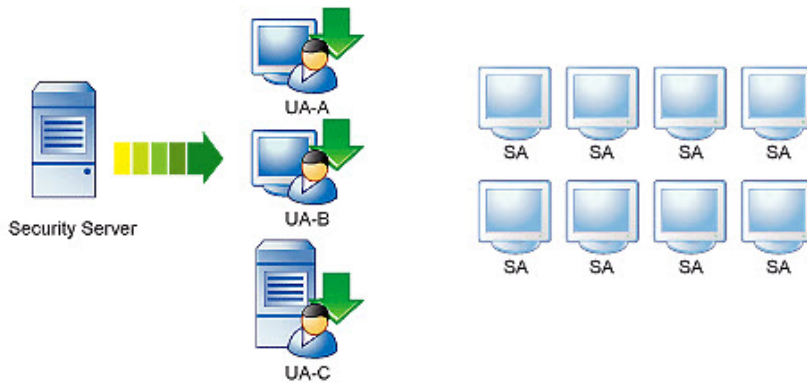
3. The Security Server then notifies the Security Agents that updated components are available.

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.

Update Agent Order Table	
IP Range	Update Agent
10.1.1.1-10.1.1.10	UA-A
10.2.1.1-10.2.1.10	UA-B
10.3.1.1-10.3.1.10	UA-C

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.
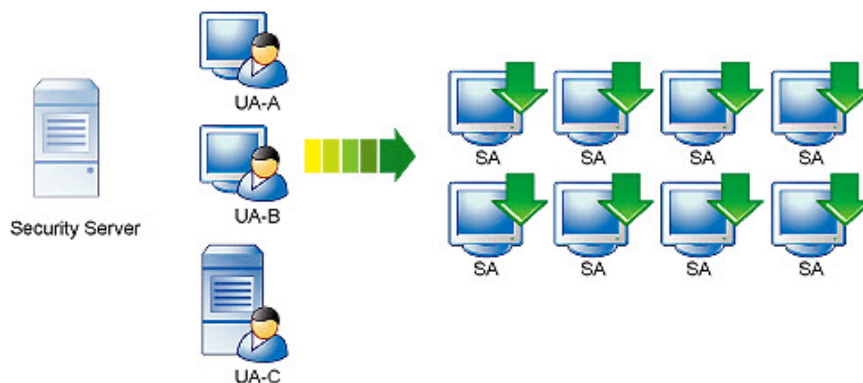
Configuring Update Agents

Procedure

1. Navigate to **Updates** > **Source**.

2. Click the **Update Agents** tab.

3. Perform the following tasks:

Task	Steps
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.

Task	Steps
Configure Security Agents to update from Update Agents	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.

Task	Steps
Remove Update Agents	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**. 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.
Unassign Security Agents from Update Agents	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.

VARIABLE	DESCRIPTION
{$CSM_SERVERNAME}	The name of the Security Server that manages the agents

Variable	Description
%CV	Number of incidents
%CU	The time unit (minutes, hours)
%CT	Number of %CU
%CP	Percentage of total email messages that is spam

The following is an example notification:

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

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

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 threat outbreak in your organization.

Configuring Outbreak Defense

Procedure

1. Go to **Outbreak Defense**.

2. In the **Status of Device(s) within Outbreak Defense Enforcement** section, click **Configure Outbreak Defense**.

3. To turn on Outbreak Defense, select **Enable Outbreak Defense for Yellow Alerts**.

4. The option **Notify client users when Outbreak Defense starts** is automatically selected. Clear the checkbox if you do not want to send Outbreak Defense notifications to users.

5. By default, **Disable Outbreak Defense** is set to 2 days. The period of time can be extended to up to 30 days.

6. Update the following as required:

OPTION	DESCRIPTION
Limit/deny access to shared folders	Select this option to limit or deny access to shared network folders as part of your Outbreak Defense strategy. Choose one of the following: • **Allow read access only** • **Deny full access**
Block ports	Select this option to block ports as part of your Outbreak Defense strategy. Choose one of the following: • **All ports** • **Specified ports**

OPTION	DESCRIPTION
	If you chose **Specified ports** click **Add** and select one of the following: • **Commonly used ports**: select the port(s) from the list • **Ports common used by Trojan programs**: there are 40 or more ports know to be used by Trojan programs • **A port number between 1 and 65535, or a port range**: define the port or port range • **Ping protocol (ICMP)**
Deny write access to files and folders	Select this option to deny write access to specific files and folders. Choose from the following: • **Files to protect for specific directories**: type the directory path and then specify whether to deny write access to all files or just specific file types • **Files to protect for all directories**: type the name of the specific file(s) to protect (including the file extension)
Deny access to all executable compressed files	Select this option to deny access to executable compressed files (packers). Specify whether to allow access to trusted files created by the supported executable packer programs.

7. Click **Save**.

Outbreak Defense Current Status

Navigate to **Live Status** > **Outbreak Defense** to view the Outbreak Defense status.

Outbreak Defense for Yellow Alert

This section of the page displays information about Outbreak Defense Yellow Alerts:

• **Start Time**: The time when a Yellow Alert was activated by an administrator.

• **Outbreak Defense activated**: The number of computers for which Outbeak Defense was activated. Click the hyperlinked number to go to the Outbreak Defense page.

- **Outbreak Defense de-activated**: The number of computers for which Outbreak Defense was de-activated. Click the hyperlinked number to go to the Outbreak Defnese page.

Action Required

This section of the page displays information about vulnerable computers and computers requiring cleaning:

- **Vulnerable computers**: The number of computers that have vulnerabilities.

- **Computers to clean**: The number of computers awaiting cleanup.

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.

Configuring Vulnerability Assessment

Procedure

1. Go to **Outbreak Defense**.

2. In the **Vulnerable Computer(s)** section, click **Configure Scheduled Assessment**.

3. To turn on scheduled vulnerability assessments, select **Enable scheduled vulnerability prevention**.

4. In the **Schedule** section, select the frequency of vulnerability assessments:

   - **Daily**

   - **Weekly**

   - **Monthly**

   - **Start Time**

5. In the **Target** section, select the group(s) that you want to assess for vulnerabilities:

   - **All groups**: All groups in the Security Group Tree

   - **Specified groups**: Server or desktop groups in the Security Group Tree

6. Click **Save**.

Running On-Demand Vulnerability Assessments

Procedure

1. Go to **Outbreak Defense**.

2. In the **Vulnerability Computer(s)** section, click **Scan for Vulnerabilities Now**.

3. Click **OK** to run the vulnerability scan.

    The **Vulnerability Scan Notification Progress** dialog displays. When the scan is complete the **Vulnerability Scan Notification Results** dialog displays.

4. Review the scan results in the **Vulnerability Scan Notification Results** dialog, then click **Close**.

Damage Cleanup

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 On-Demand Clean Up

Procedure

1. Go to **Outbreak Defense**.

2. In the **Computer(s) to Clean Up** section, click **Clean Up Now**.

    Unsuccessful clean up results occur when a Security Agent is offline, or in unexpected situations such as a network interruption.

3. Click **OK** to start the clean up.

    The **Clean Up Notification Progress** dialog displays. When the clean up is complete the **Clean Up Notification Results** dialog displays.

4. Review the clean up results in the **Clean Up Notification Results** dialog, then click **Close**.

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:

SETTINGS	DESCRIPTION
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: • **Help Desk Label** • **Help Desk Email Address** • **Additional Information**: This will pop-up when the user mouses over the label

SETTINGS	DESCRIPTION
General Scan Settings	• **Disable Smart Scan service**: 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** > **{Group}** > **Configure** > **Scan Method**. 📝 **Note** For guidelines on switching Security Agents between scan methods, see *Configuring Scan Methods on page 5-5*. • **Enable deferred scanning on file operations**: Enable this setting to temporarily improve system performance. ⚠️ **WARNING!** Enabling deferred scanning can create security risks. • **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. • **Exclude the Security Server database folder**: 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. • **Exclude the Microsoft Exchange server folders when installed on Microsoft Exchange Server**: Prevents Agents installed on the Microsoft Exchange server from scanning Microsoft Exchange folders. • **Exclude the Microsoft domain control folders**: Prevents Agents installed on the Domain Controller from scanning Domain Controller folders. These folders store user information, user names, passwords, and other important information.

Settings	Description
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	• **Scan for cookies**: The Security Agent scand for cookies. • **Add cookie detections to the Spyware log**: Adds each detected spyware cookie to the spyware log.
Firewall Settings	Select the **Disable Firewall and uninstall drivers** check box to uninstall the WFBS client firewall and 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.

SETTINGS	DESCRIPTION
Web Reputation and URL Filtering	• **Approved List**: Websites (and their sub-domains) excluded from Web Reputation and URL Filtering verifications. **Note** The approved list takes precedence over the blocked list. When a URL matches an entry in the approved list, agents always allow access to the URL, even if it is in the blocked list. Enabling Approved or Blocked Lists for a specific group, overrides the Global Approved or Blocked Settings for the group. • **Blocked List**: Websites (and their sub-domains) that are always blocked during 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. • **IP Exception List**: IP addresses (e.g. 192.168.0.1) excluded from Web Reputation and URL Filtering verifications. Type critical IP addresses that your organization deems trustworthy. • **Send Web Reputation and URL Filtering logs to the Security Server**

SETTINGS	DESCRIPTION
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.
Security Agent Uninstallation Password	• **Allow the client user to uninstall Security Agent without a password.** • **Require a password for the client user to uninstall Security Agent.**
Security Agent Program Exit and Unlock Password	• **Allow the client users to exit and unlock the Security Agent on their computer without a password.** • **Require client users to enter a password to exit and unlock the Security Agent.** **Note** Unlocking the Security Agent allows the user to override all settings configured under **Security Settings** > **{group}** > **Configure** > **Client Privileges**.
Preferred IP Address	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: • **IPv4 first, then IPv6**: 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. • **IPv6 first, then IPv4**: 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.

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:

Settings	Description
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	DESCRIPTION
Quarantine Maintenance	By default, Security Agents send quarantined infected files to the following directory in the Security Server: <Security Server installation folder>\PCCSRV\Virus If you need to change the directory (for example, if it has insufficient disk space), type an absolute path, such as D:\Quarantined Files, in the **Quarantine Directory** field. If you do this, be sure to also apply the same changes in **Security Settings** > **{Group}** > **Configure** > **Quarantine** or agents will continue sending the files to <Security Server installation folder>\PCCSRV\Virus. In addition, configure the following maintenance settings: • **Quarantine folder capacity**: The size of the quarantine folder in MB. • **Maximum size for a single file**: The maximum size of a single file stored in the quarantine folder in MB. • **Delete All Quarantined Files**: Deletes all files in the Quarantine folder. If the folder is full and a new file is uploaded, the new file will not be stored. If you do not want agents to send quarantined files to the Security Server, configure the new directory in **Security Settings** > **Configure** > **Quarantine** and ignore all the maintenance settings. See *Quarantine Directory on page 5-30* for instructions.
Security Agent Installation	**Security Agent Installation directory**: During installation, you are prompted to type the Security Agent installation directory, which is where Setup installs each Security Agent. 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. Use one of the following variables to set the installation path: • `$BOOTDISK`: The drive letter of the boot disk • `$WINDIR`: The folder where Windows is installed • `$ProgramFiles`: The programs folder

3. Click **Save**.

Chapter 12

Using Logs and Reports

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

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

TYPE (ENTITY THAT GENERATED THE LOG ENTRY)	CONTENT (TYPE OF LOG TO OBTAIN CONTENT FROM)
Management console events	• Manual Scan (launched from the web console) • Update (Security Server updates) • Outbreak Defense events • Console events

Type (entity that generated the log entry)	Content (type of log to obtain content from)

Desktop/Server	• Virus logs
	    • Manual Scan
	    • Real-time Scan
	    • Scheduled scan
	    • Cleanup
	• Spyware/Grayware logs
	    • Manual Scan
	    • Real-time Scan
	    • Scheduled scan
	• Web Reputation logs
	• URL Filtering logs
	• Behavior monitoring logs
	• Update logs
	• Network virus logs
	• Outbreak Defense logs
	• Event logs
	• Device Control logs
	• Hot Fix Deployment logs

TYPE (ENTITY THAT GENERATED THE LOG ENTRY)	CONTENT (TYPE OF LOG TO OBTAIN CONTENT FROM)
Exchange server (Advanced only)	• Virus logs
	• Attachment Blocking logs
	• Content Filtering/Data Loss Prevention logs
	• Update logs
	• Backup logs
	• Archive logs
	• Outbreak Defense logs
	• Scan Event logs
	• Unscannable Message Parts logs
	• Web Reputation logs
	• Mobile Event logs

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.

  - **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:

Task	Steps

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*.

Task	Steps
Delete reports	a. Select the row containing the report links. b. Click **Delete**. --- **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	STEPS
Create a scheduled report template	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**.

Task	Steps
View scheduled reports	a. On the row containing the template from which the scheduled reports are generated, click **Report History**. A new screen opens. 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. 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*.
Template Maintenance Tasks	
Edit template settings	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.
Enable/Disable a template	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.

Task	Steps
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	
Send a link to the scheduled reports	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. --- **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.

Task	Steps
Delete scheduled reports	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 click **Delete**. --- **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

REPORT ITEM	DESCRIPTION
Antivirus	**Desktop/Servers Virus Summary** Virus reports show detailed information about the numbers and types of virus/malware that the scan engine detected and the actions it took against them. The report also lists the Top virus/malware names. Click the names of the virus/malware to open a new web browser page and redirect it to the Trend Micro virus encyclopedia to learn more about that virus/malware.
	Top 5 Desktop/Servers with Virus Detections Displays the top five desktops or servers reporting virus/malware detections. Observing frequent virus/malware incidents on the same client might indicate that a client represents a high security risk that might require further investigation
Outbreak Defense History	**Outbreak Defense History** Displays recent outbreaks, the severity of the outbreaks, and identifies the virus/malware causing the outbreak and how it was delivered (by email or file).
Anti-spyware	**Desktop/Servers Spyware/Grayware Summary** The spyware/grayware report shows detailed information about the spyware/grayware threats detected on clients, including the number of detections and the actions that WFBS took against them. The report includes a pie chart that shows the percentage of each anti-spyware scan action that has been performed.
	Top 5 Desktop/Servers with Spyware/Grayware Detections The report also shows the top five spyware/grayware threats detected and the five desktops/servers with the highest number of spyware/grayware detected. To learn more about the spyware/grayware threats that have been detected, click the spyware/grayware names. A new web browser page opens and displays related information on the spyware/grayware on the Trend Micro website.

Report Item	Description
Anti-spam summary (Advanced only)	**Spam Summary** Anti-spam reports show information about the number of spam and phish detected among the total amount of messages scanned. It lists the reported false positives.
Web Reputation	**Top 10 Computers Violating Web Reputation Policies**
URL category	**Top 5 URL Category Policies Violated** Lists the most commonly accessed website categories that violated the policy.
	Top 10 Computers Violating URL Category Policies
Behavior Monitoring	**Top 5 Programs Violating Behavior Monitoring Policies**
	Top 10 Computers Violating Behavior Monitoring Policies
Device Control	**Top 10 Computer Violating Device Control Policy**
Content filtering summary (Advanced only)	**Content Filtering Summary** Content filtering reports show information about the total number of messages that the Messaging Security Agent filtered.
	Top 10 Content Filtering Rules Violated A list of the top 10 content filtering rules violated. Use this feedback to fine-tune your filtering rules.
Network Virus	**Top 10 Network Viruses Detected** Lists the 10 network viruses most frequently detected by the common firewall driver. Click the names of the viruses to open a new web browser page and redirect it to the Trend Micro virus encyclopedia to learn more about that virus.
	Top 10 Computers Attacked List the computers on your network that report the most frequent virus incidents.

Performing Maintenance Tasks for Reports and Logs

Procedure

1. Navigate to **Reports** > **Maintenance**.

2. Perform the following tasks:

TASK	STEPS
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

LICENSE TYPE	ACTIVATION CODE
Fully licensed version of WFBS Standard	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx
Fully licensed version of WFBS Advanced	CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

> **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 1-19*.

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

1. Stop the Trend Micro Security Server Master Service.

2. Manually copy the following files and folders from the folder to an alternate location:

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

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

- ofcscan.ini: Contains global settings.

- ous.ini: Contains the update source table for antivirus component deployment.

- • Private folder: Contains firewall and update source settings.

- • Web\TmOPP folder: Contains Outbreak Defense settings.

- • Pccnt\Common\OfcPfw.dat: Contains firewall settings.

- • Download\OfcPfw.dat: Contains firewall deployment settings.

- • Log folder: Contains system events and the verify connection log.

- • Virus folder: The folder in which WFBS quarantines infected files.

- • HTTDB folder: Contains the WFBS database.

3. Uninstall the Security Server. See *Uninstalling the Security Server on page 13-8*.

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=xxxxxx 0 0
      ```

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

      \Private\component.ini

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

7. With the backups you created, overwrite the WFBS database and the relevant files and folders on the target machine in the PCCSRV folder.

8. Restart the Trend Micro Security Server Master Service.

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.

Uninstalling the Trend Micro Security Server does not uninstall Agents. Administrators must uninstall or move all Agents to another Security Server before uninstalling the Trend Micro Security Server. See *Removing Agents on page 3-38*.

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 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 3-15*.

    - **Restore Encrypted Virus and Sypware** (VSEncode.exe): Opens infected files encrypted by WFBS. See *Restoring Encrypted Files on page 14-9*.

    - **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** (WFBS_WIN_All_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 3-41*.

- **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 14-13*.

✎ 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 Remote Manager Agent

The Trend Micro Remote Manager Agent allows resellers to manage WFBS with Trend Micro Remote Manager (TMRM). The TMRM Agent (version 3.5) is installed on Security Server 9.0 SP1.

If you are a Trend Micro certified partner, you can install the agent for Trend Micro Remote Manager (TMRM). If you chose not to install the TMRM agent after the Security Server installation completes, you can do so later.

Installation requirements:

- TMRM Agent GUID

  To obtain the GUID, open the TMRM 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 TMRMAgentforWFBS.exe.

   For example: C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility \RmAgent\TMRMAgentforWFBS.exe

   > **Note**
   >
   > Skip this step if you are launching the installation from the Security Server Setup screen.

2. In the Trend Micro 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 Trend Micro Remote Manager account and I want to install the agent**. Click **Next**.

5. Determine your scenario.

SCENARIO	STEPS
New customer	a. Select **Associate with a new customer**. b. Click **Next**. Enter the customer information. > **Note** > If the customer already exists on the TMRM 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 TMRM network tree. To avoid this, use the method below.

SCENARIO	STEPS
Existing customer	a. Select **This product already exists in Remote Manager**.
	Note WFBS must already have been added to the TMRM Console. See your TMRM 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 TMRM Agent should automatically register to the Trend Micro Remote Manager server. The Agent should show as Online on the TMRM 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*

Procedure

1. On the Security Server, go to the following directory:

   {Server Installation Folder}\PCCSRV\Admin\Utility\

2. Double-click **TMDiskCleaner.exe**.

   The Trend Micro Worry-Free Business Security Disk Cleaner appears.

   > **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

1. On the Security Server, open a Command Prompt window.

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 an infected file 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

FILE	DESCRIPTION
Quarantined files on the client	These files are found in the following directories: • <Security Agent installation folder>\SUSPECT\Backup or <Security Agent installation folder>\quarantine, whichever is available. • <Messaging Security Agent installation folder>\storage\quarantine These files are uploaded to the designated quarantine directory, which is typically a directory on the Security Server.
Quarantined files on the designated quarantine directory	By default, this directory is located on the Security Server computer (<Security Server installation folder>\PCCSRV\Virus). To change the directory, navigate to **Preferences** > **Global Settings** > **System** tab and go to the Quarantine Maintenance section.
Backed up encrypted files	These are the backup of infected files that agents were able to clean. These files are found in the following folders: • <Security Agent installation folder>\Backup • <Messaging Security Agent installation folder>\storage\backup To restore these files, users need to move them to the quarantine directory on the client.

> ⚠ **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.

   Administrators can restore files classified as spyware/grayware from the Spyware/Grayware tab. The screen displays a list of files found under: <Security Agent installation folder>\BackupAS.

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:

   ```
   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 14-2. Restore Parameters

PARAMETER	DESCRIPTION
None (no parameter)	Encrypt files
/d	Decrypt files
/debug	Create a debug log and save it to the computer. On the client, the debug log VSEncrypt.log is created in the <Agent installation folder>.
/o	Overwrite an encrypted or decrypted file if it already exists
/f <filename>	Encrypt or decrypt a single file
/nr	Do not restore the original file name
/v	Display information about the tool
/u	Launch the tool's user interface
/r <Destination folder>	The folder where a file will be restored
/s <Original file name>	The file name of the original encrypted file

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_WIN_All_ReGenID.exe to a temporary folder on the client where the Security Agent is installed.

    Example: C:\temp

3. Double-click WFBS_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 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

- Windows Server 2012 R2 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 2012/2012 R2 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.

2. Under the **Security** tab, click **Trend Micro Worry-Free Business Security** to view the status information.

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:
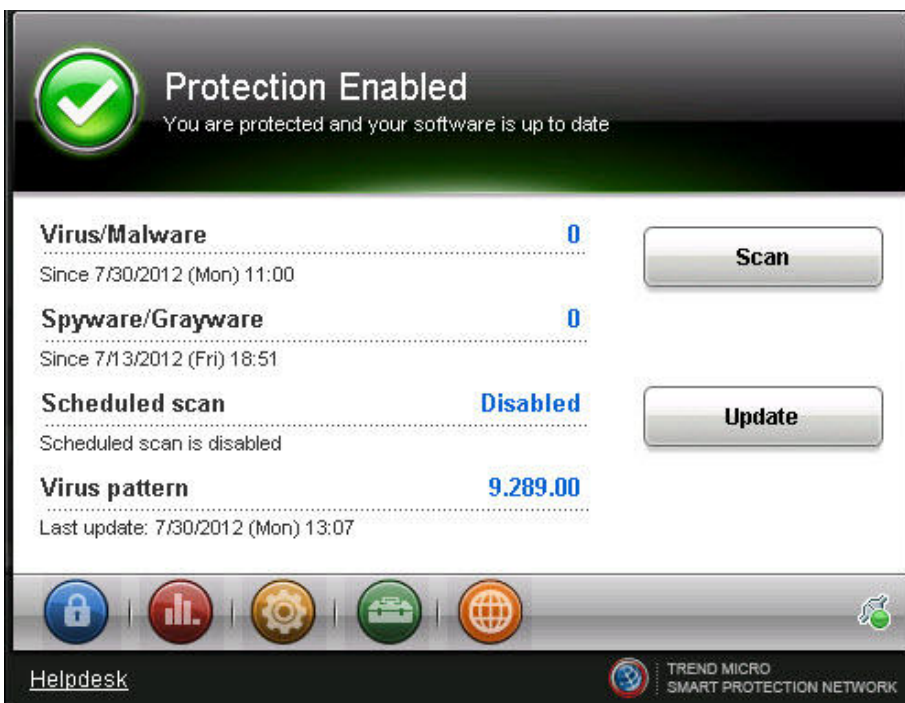
The following table lists the icons and their meanings on the Security Agent Console Main User Interface:

TABLE A-1. Security Agent Console Main User Interface icons

| ICON	STATUS	EXPLANATION AND ACTION
	Protection Enabled: You are protected and your software is up to date	The software is up-to-date and running properly. No action is required.
	Restart Computer: Restart the computer to finish fixing security threats	Security Agent has discovered threats that it cannot fix immediately. Restart the computer to finish fixing these threats.
	Protection at Risk: Contact your administrator	Real-time Scan is disabled or protection is at risk for another reason. Enable Real-time Scan and if this does not solve the problem, contact Support.
	Update Now: You have not received an update in (number) days.	The virus pattern is older than 3 days. Update the Security Agent immediately.
	Smart Scan Not Available: Check your Internet connection	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.
	Restart Computer: Restart your computer to finish installing an update	Restart your computer to finish an update.
	Updating Program: Your security software is updating	An update is in progress. Do not disconnect from the network until finished.

Viewing Security Agent Icons on the Windows Task Bar

The following Security Agent icons will display on the client's Windows Task Bar:

ICON	MEANING
	Status is normal
	(Animated) A Manual Scan or Scheduled Scan is running. The Security Agent is using Conventional Scan or Smart Scan.
	The Security Agent is performing an update.
	Action is necessary:
	• Real-time Scan is disabled
	• Reboot required in order to fully clean malware
	• Reboot required due to an updated engine
	• Update is necessary
	Note Open the Security Agent Main Console to see what action is required.

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.
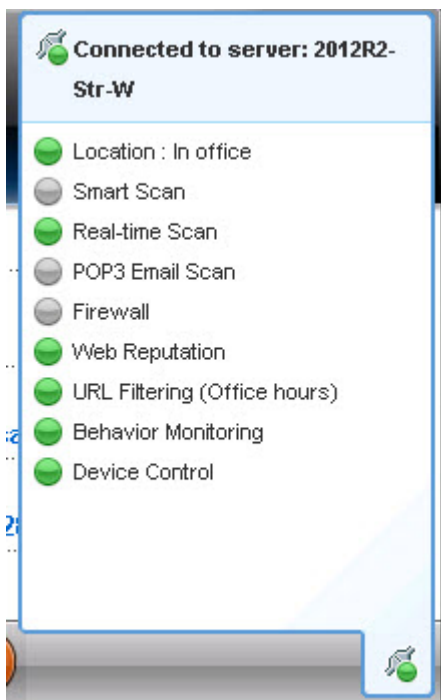
The following table lists the Console Flyover icons and their meanings:

TABLE A-2. Console Flyover Icons

FEATURE	ICON	MEANING
Connection		Connected to the Security Server
		Not connected to the 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 **Update Now**.

Feature	Icon	Meaning
Real Time Scan		On
		Off
Smart Scan		Connected to Trend Micro Smart Protection Network
		Unable to connect to the Smart Protection Network; protection is reduced as Security Agents are unable to send scan queries. **Note** Verify that the Smart Scan service TMiCRCScanService is running and that Security Agents are connected to the Security Server.
		Smart Scan is disabled. Using Conventional Scan
• Firewall • Web Reputation • URL Filtering • Behavior Monitoring • Device Control		On
		Off

Appendix B

IPv6 Support in WFBS

This appendix is required reading for users who plan to deploy WFBS in an environment that supports IPv6 addressing. This appendix contains information on the extent of IPv6 support in WFBS.

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 WFBS and Security Agents

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

ITEM	LIMITATION
Agent management	A pure IPv6 server cannot: • Deploy agents to pure IPv4 clients • Manage pure IPv4 agents.
Updates and centralized management	A pure IPv6 server cannot update from pure IPv4 update sources, such as: • Trend Micro ActiveUpdate Server • Any pure IPv4 custom update source
Product registration, activation, and renewal	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.
Proxy connection	A pure IPv6 server cannot connect through a pure IPv4 proxy server.
Plug-in solutions	A pure IPv6 server will have Plug-in Manager but will not be able to deploy any of the plug-in solutions to: • Pure IPv4 agents or pure IPv4 hosts (because of the absence of a direct connection) • Pure IPv6 agents or pure IPv6 hosts because none of the plug-in solutions support IPv6.

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 Security Agent Limitations

The following table lists the limitations when the Security Agent only has an IPv6 address.

TABLE B-2. Pure IPv6 Security Agent Limitations

ITEM	LIMITATION
Parent Security Server	Pure IPv6 agents cannot be managed by a pure IPv4 Security Server.
Updates	A pure IPv6 Security Agent cannot update from pure IPv4 update sources, such as: • Trend Micro ActiveUpdate Server • A pure IPv4 Security Server • A pure IPv4 Update Agent • Any pure IPv4 custom update source
Scan queries and Smart Feedback	A pure IPv6 Security Agent cannot send queries to Trend Micro Smart Protection Network and cannot use Smart Feedback.
Plug-in solutions	Pure IPv6 agents cannot install plug-in solutions because none of the plug-in solutions support IPv6.
Proxy connection	A pure IPv6 Security Agent cannot connect through a pure IPv4 proxy server.

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 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.

• WFBS accepts standard IPv6 address presentations.

For example:

```
2001:0db7:85a3:0000:0000:8a2e:0370:7334
```

```
2001:db7:85a3:0:0:8a2e:370:7334
```

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- WFBS also accepts link-local IPv6 addresses, such as:

```
fe80::210:5aff:feaa:20a2
```

> ⚠️ **WARNING!**
>
> Exercise caution when specifying a link-local IPv6 address because even though WFBS can accept the address, it might not work as expected under certain circumstances. For example, Security 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. For example, for the Outside Server Management feature, the prefix length can only be between 112 (65,536 IP addresses) and 128 (2 IP addresses).

- Some settings that involve IPv6 addresses or address ranges will be deployed to Security Agents but Security Agents will ignore them. For example, if you configured the smart protection source list and included a Smart Protection Server identified by its IPv6 address, pure IPv4 Security Agents will ignore the server and connect to the other smart protection sources.

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:

http://esupport.trendmicro.com/en-us/business/default.aspx

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 Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated
	225 E. John Carpenter Freeway, Suite 1500
	Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900
	Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

    http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

    http://docs.trendmicro.com

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.

Run the tool on all platforms that WFBS supports. To obtain this tool and relevant documentation, contact your support provider.

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem

- Appliance or network information

- Computer brand, model, and any additional hardware connected to the endpoint

- Amount of memory and free hard disk space

- Operating system and service pack version

- Endpoint client version

- Serial number or activation code

- Detailed description of install environment

- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Record the case number for tracking purposes.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1055473.aspx

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"

- Correlated threat information pages to form a complete web attack story

- Internet threat advisories about targeted attacks and security threats

- Web attack and online trend information

- Weekly malware reports

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

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.

Critical Patch

A critical patch focuses on security issues suitable for deployment to all customers. Windows critical patches include a Setup program, while non-Windows patches commonly have a setup script.

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).

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 agent 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. However, this does not mean they are entirely safe. 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 WFBS 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 Security Agent. The WFBS firewall can help prevent the following well-known intrusions:

INTRUSION	DESCRIPTION
Too Big Fragment	A Denial of Service attack where a hacker directs an oversized TCP/UDP packet at a target client. This can cause the client's buffer to overflow, which can freeze or reboot the client.
Ping of Death	A Denial of Service attack where a hacker directs an oversized ICMP/ICMPv6 packet at a target client. This can cause the client's buffer to overflow, which can freeze or reboot the client.
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 targeted client. The target client 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 the client, causing the client to continually send synchronization acknowledgment (SYN/ACK) responses. This can exhaust client memory and eventually crash the client.

INTRUSION	DESCRIPTION
Overlapping Fragment	Similar to a Teardrop attack, this Denial of Service attack sends overlapping TCP fragments to the client. 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 client.
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 client'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 client, which cannot properly process the IGMP packets. This can freeze or slow down the client.
LAND Attack	A type of attack that sends IP synchronization (SYN) packets with the same source and destination address to the client, causing the client to send the synchronization acknowledgment (SYN/ACK) response to itself. This can freeze or slow down the client.

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

OPERATOR	HOW IT WORKS	EXAMPLE
any keyword	The Messaging Security Agent searches content that matches the word	Type the word and add it to the keyword list
OR	The Messaging Security Agent searches for any of the keywords separated by OR For example, apple OR orange. The agent searches for either apple or orange. If content contains either, then there is a match.	Type ".OR." between all the words you want to include For example, "apple .OR. orange"

OPERATOR	HOW IT WORKS	EXAMPLE
AND	The Messaging Security Agent searches for all of the keywords separated by AND For example, apple AND orange. The agent searches for both apple and orange. If content does not contain both, then there is no match.	Type ".AND." between all the words you want to include For example, "apple .AND. orange"
NOT	The Messaging Security Agent excludes keywords following NOT from search. For example, .NOT. juice. The agent searches for content that does not contain juice. If the message has "orange soda", there is a match, but if it contains "orange juice", there is no match.	Type ".NOT." before a word you want to exclude For example, ".NOT. juice"
WILD	The wildcard symbol replaces a missing part of the word. Any words that are spelled using the remaining part of the wildcard are matched. 📝 **Note** The Messaging Security Agent does not support using "?" in the wildcard command ".WILD.".	Type ".WILD." before the parts of the word you want to include For example, if you want to match all words containing "valu", type ".WILD.valu". The words Valumart, valucash, and valubucks all match.
REG	To specify a regular expression, add a .REG. operator before that pattern (for example, .REG. a.*e). See *Regular Expressions on page D-10*.	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-10*.

- 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 D-2. How to Use Keywords

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

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

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:

http://www.perl.com/doc/manual/html/pod/perlre.html

⚠️ **WARNING!**

Regular expressions are a powerful string matching tool. For this reason, Trend Micro recommends that Administrators who choose to use regular expressions be familiar and comfortable with regular expression syntax. Poorly written regular expressions can have a dramatic negative performance impact. Trend Micro recommends is to start with simple regular expressions that do not use complex syntax. When introducing new rules, use the archive action and observe how the 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

ELEMENT	WHAT IT MEANS	EXAMPLE
.	The dot or period character represents any character except new line character.	do. matches doe, dog, don, dos, dot, etc. d.r matches deer, door, etc.
*	The asterisk character means zero or more instances of the preceding element.	do* matches d, do, doo, dooo, doooo, etc.

Element	What it Means	Example
+	The plus sign character means one or more instances of the preceding element.	do+ matches do, doo, dooo, doooo, etc. but not d
?	The question mark character means zero or one instances of the preceding element.	do?g matches dg or dog but not doog, dooog, etc.
( )	Parenthesis characters group whatever is between them to be considered as a single entity.	d(eer)+ matches deer or deereer or deereereer, etc. The + sign is applied to the substring within parentheses, so the regex looks for d followed by one or more of the grouping "eer."
[ ]	Square bracket characters indicate a set or a range of characters.	d[aeiouy]+ matches da, de, di, do, du, dy, daa, dae, dai, etc. The + sign is applied to the set within brackets parentheses, so the regex looks for d followed by one or more of any of the characters in the set [aeioy]. d[A-Z] matches dA, dB, dC, and so on up to dZ. The set in square brackets represents the range of all upper-case letters between A and Z.
[^]	Carat characters within square brackets logically negate the set or range specified, meaning the regex will match any character that is not in the set or range.	d[^aeiouy] matches db, dc or dd, d9, d#--d followed by any single character except a vowel.

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

TABLE D-4. Character Classes (shorthand)

ELEMENT	WHAT IT MEANS	EXAMPLE
\d	Any digit character; functionally equivalent to [0-9] or [[:digit:]]	\d matches 1, 12, 123, etc., but not 1b7--one or more of any digit characters.
\D	Any non-digit character; functionally equivalent to [^0-9] or [^[:digit:]]	\D matches a, ab, ab&, but not 1--one or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.
\w	Any "word" character--that is, any alphanumeric character; functionally equivalent to [_A-Za-z0-9] or [_[:alnum:]]	\w matches a, ab, a1, but not !&--one or more upper- or lower-case letters or digits, but not punctuation or other special characters.
\W	Any non-alphanumeric character; functionally equivalent to [^_A-Za-z0-9] or [^_[:alnum:]]	\W matches *, &, but not ace or a1--one or more of any character but upper- or lower-case letters and digits.
\s	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [[:space]]	vegetable\s matches "vegetable" followed by any white space character. So the phrase "I like a vegetable in my soup" would trigger the regex, but "I like vegetables in my soup" would not.

Element	What it Means	Example
\S	Any non-white space character; anything other than a space, new line, tab, non-breaking space, etc.; functionally equivalent to [^[:space]]	vegetable\S matches "vegetable" followed by any non-white space character. So the phrase "I like vegetables in my soup" would trigger the regex, but "I like a vegetable in my soup" would not.

Table D-5. Character Classes

Element	What it Means	Example
[:alpha:]	Any alphabetic characters	.REG. [[:alpha:]] matches abc, def, xxx, but not 123 or @#$.
[:digit:]	Any digit character; functionally equivalent to \d	.REG. [[:digit:]] matches 1, 12, 123, etc.
[:alnum:]	Any "word" character--that is, any alphanumeric character; functionally equivalent to \w	.REG. [[:alnum:]] matches abc, 123, but not ~!@.
[:space:]	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to \s	.REG. (vegetable)[[:space:]] matches "vegetable" followed by any white space character. So the phrase "I like a vegetable in my soup" would trigger the regex, but "I like vegetables in my soup" would not.
[:graph:]	Any characters except space, control characters or the like	.REG. [[:graph:]] matches 123, abc, xxx, ><", but not space or control characters.
[:print:]	Any characters (similar with [:graph:]) but includes the space character	.REG. [[:print:]] matches 123, abc, xxx, ><", and space characters.
[:cntrl:]	Any control characters (e.g. CTRL + C, CTRL + X)	.REG. [[:cntrl:]] matches 0x03, 0x08, but not abc, 123, !@#.
[:blank:]	Space and tab characters	.REG. [[:blank:]] matches space and tab characters, but not 123, abc, !@#

ELEMENT	WHAT IT MEANS	EXAMPLE
[:punct:]	Punctuation characters	.REG. [[:punct:]] matches ; : ? ! ~ @ # $ % & * ' " , etc., but not 123, abc
[:lower:]	Any lowercase alphabetic characters (Note: 'Enable case sensitive matching' must be enabled or else will function as [:alnum:])	.REG. [[:lower:]] matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, !@#.
[:upper:]	Any uppercase alphabetic characters (Note: 'Enable case sensitive matching' must be enabled or else it will function as [:alnum:])	.REG. [[:upper:]] matches ABC, DEF, STRESS, DO, etc., but not abc, Def, Stress, Do, 123, !@#.
[:xdigit:]	Digits allowed in a hexadecimal number (0-9a-fA-F)	.REG. [[:xdigit:]] matches 0a, 7E, 0f, etc.

TABLE D-6. Pattern Anchors

ELEMENT	WHAT IT MEANS	EXAMPLE
^	Indicates the beginning of a string.	^(notwithstanding) matches any block of text that began with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would trigger the regex, but "The fact that I like vegetables in my soup notwithstanding" would not.
$	Indicates the end of a string.	(notwithstanding)$ matches any block of text that ended with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would not trigger the regex, but "The fact that I like vegetables in my soup notwithstanding" would.

TABLE D-7. Escape Sequences and Literal Strings

ELEMENT	WHAT IT MEANS	EXAMPLE
\	In order to match some characters that have special meaning in regular expression (for example, "+").	(1) .REG. C\\C\+\+ matches 'C\C ++'. (2) .REG. * matches *. (3) .REG. \? matches ?.
\t	Indicates a tab character.	(stress)\t matches any block of text that contained the substring "stress" immediately followed by a tab (ASCII 0x09) character.
\n	Indicates a new line character. **Note** Different platforms represent a new line character. On Windows, a new line is a pair of characters, a carriage return followed by a line feed. On Unix and Linux, a new line is just a line feed, and on Macintosh a new line is just a carriage return.	(stress)\n\n matches any block of text that contained the substring "stress" followed immediately by two new line (ASCII 0x0A) characters.
\r	Indicates a carriage return character.	(stress)\r matches any block of text that contained the substring "stress" followed immediately by one carriage return (ASCII 0x0D) character.

ELEMENT	WHAT IT MEANS	EXAMPLE
\b	Indicates a backspace character. OR Denotes boundaries.	(stress)\b matches any block of text that contained the substring "stress" followed immediately by one backspace (ASCII 0x08) character. A word boundary (\b) is defined as a spot between two characters that has a \w on one side of it and a \W on the other side of it (in either order), counting the imaginary characters off the beginning and end of the string as matching a \W. (Within character classes \b represents backspace rather than a word boundary.) For example, the following regular expression can match the social security number: .REG. \b \d{3}-\d{2}-\d{4}\b
\xhh	Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).	\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.

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

.REG. \b\d{3}-\d{2}-\d{4}\b	
333-22-4444	Match
333224444	Not a match
333 22 4444	Not a match
3333-22-4444	Not a match

333-22-44444	Not a match

If you modify the expression as follows,

[Format] .REG. \b\d{3}\x20\d{2}\x20\d{4}\b

the new expression matches the following sequence:

333 22 4444

Scan 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

PRODUCT NAME	INSTALLATION PATH LOCATION
InterScan eManager 3.5x	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager \CurrentVersion ProgramDirectory=
ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion ProgramDirectory=
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=

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

PRODUCT NAME	INSTALLATION PATH LOCATION
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

PRODUCT NAME	INSTALLATION PATH LOCATION
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder=

PRODUCT NAME	INSTALLATION PATH LOCATION
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:

Microsoft Exchange exclusions	
Microsoft Exchange Server Database	C:\Program Files\Exchsrvr\MDBDATA
Microsoft Exchange MTA files	C:\Program Files\Exchsrvr\Mtadata
Microsoft Exchange Message tracking log files	C:\Program Files\Exchsrvr\server_name.log
Microsoft Exchange SMTP Mailroot	C:\Program Files\Exchsrvr\Mailroot
Microsoft Exchange working files	C:\Program Files\Exchsrvr\MDBDATA
Site Replication Service	C:\Program Files\Exchsrvr\srsdata
	C:\Program Files\Exchsrvr\conndata
IIS Exclusions	
IIS System Files	C:\WINDOWS\system32\inetsrv
IIS Compression Folder	C:\WINDOWS\IIS Temporary Compressed Files

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

Windows SharePoint Services Exclusions	
Temporary SharePoint folder	C:\windows\temp\FrontPageTempDir

Client Desktop Folder Exclusions	
Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore

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

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 clients. During an outbreak, WFBS blocks the following port numbers that Trojan programs may use.

TABLE D-10. Trojan Ports

PORT NUMBER	TROJAN HORSE PROGRAM	PORT NUMBER	TROJAN HORSE PROGRAM
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver

Port Number	Trojan Horse Program	Port Number	Trojan Horse Program
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Uncleanable Files

The Virus Scan Engine is unable to clean the following files:

TABLE D-11. Uncleanable File Solutions

Uncleanable File	Explanation and Solution
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 Damage Cleanup Engine and Damage Cleanup Template remove Trojans.
Files infected with worms	A worm is a self-contained program (or set of programs) able to spread functional copies of itself or its segments to other client systems. The propagation usually takes place through network connections or email attachments. Worms are uncleanable because the file is a self-contained program.

Uncleanable File	Explanation and Solution
	Solution: Trend Micro recommends deleting worms.
Write-protected infected files	Solution: Remove the write-protection which allows for the cleaning of the file.
Password-protected files	Password-protected files include password-protected compressed files or password-protected Microsoft Office files.
	Solution: Remove the password protection which allows for the cleaning of the file.
Backup files	Files with the RB0~RB9 extensions are backup copies of infected files. The cleaning process creates a backup of the infected file in case the virus/malware damaged the file during the cleaning process.
	Solution: If successfully cleaned, you do not need to keep the backup copy of the infected file. If the client functions normally, you can delete the backup file.
Infected files in the Recycle Bin	The system may not allow the removal of infected files from 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 client 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.

	4. Type the following to delete the files:
	
	```cd \```
	```cd recycled```
	```del *.* /S```
	
	The last command deletes all files in the Recycle Bin.

	5. Check if the files were removed.

UNCLEANABLE FILE	EXPLANATION AND SOLUTION

	Solution on other operating systems (or those without NTFS):
	
	1. Restart the client in MS-DOS mode.
	2. Open the command prompt.
	3. Type the following to delete the files:
	
	`cd \`
	
	`cd recycled`
	
	`del *.* /S`
	
	The last command deletes all files in the Recycle Bin.

Infected files in Windows Temp Folder or Internet Explorer Temporary Folder	The system may not allow the cleaning of infected files in the Windows Temp folder or the Internet Explorer temporary folder because the client uses them. The files to clean may be temporary files needed for Windows operation.

	Solution on Windows XP or Windows Server 2003 with NTFS File System:
	
	1. Log on to the client 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 clients 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.

UNCLEANABLE FILE	EXPLANATION AND SOLUTION
	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 clients 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.
	Solution on other operating systems (or those without NTFS):
	1. Restart the client in MS-DOS mode.
	2. 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 clients 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.
	c. Restart the client in normal mode.
	3. 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

UNCLEANABLE FILE	EXPLANATION AND SOLUTION
	name>\Local Settings\Temporary Internet Files for Windows XP or Windows Server 2003 clients 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. Restart the client in normal mode.
Files compressed using an unsupported compression format	Solution: Uncompress the files.
Locked files or files that are currently executing	Solution: Unlock the files or wait until the files have been executed.
Corrupted files	Solution: Delete the files.

Index

T

Teardrop, D-5
test virus, 1-22
Tiny Fragment Attack, D-5
Too Big Fragment, D-4
TrendLabs, C-5
Trend Micro
    Knowledge Base, C-2
Trojan horse program, 1-21, 8-7

U

uninstallation
    using the uninstallation program, 3-40
Update Agent, 3-5

V

VBScript virus, 1-22
virus/malware, 1-21, 1-22
    ActiveX malicious code, 1-22
    boot sector virus, 1-22
    COM and EXE file infector, 1-22
    Java malicious code, 1-22
    joke program, 1-21
    macro virus, 1-22
    packer, 1-22
    probable virus/malware, 1-21
    test virus, 1-22
    Trojan horse program, 1-21
    types, 1-21, 1-22
    VBScript, JavaScript or HTML virus, 1-22
    worm, 1-22
Virus Cleanup Template, 8-7
Virus Encyclopedia, 1-21
Virus Pattern, 8-6, 8-14
Virus Scan Engine, 8-5
Vulnerability Scanner, 3-10, 3-21

computer description retrieval, 3-30
    DHCP settings, 3-24
    ping settings, 3-31

W

web console, 2-4, 2-5
    about, 2-4
    requirements, 2-5
web install page, 3-8, 3-9
web reputation, 1-17, 3-4
WFBS
    documentation, xii
worm, 1-22

www.**trendmicro**.com