



Client Server Security3

for Small and Medium Business



Administrator's Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

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

NOTE: A license to the Trend Micro Software includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Thereafter, you must renew Maintenance on an annual basis by paying Trend Micro's then-current Maintenance fees to have the right to continue receiving product updates, pattern updates, and basic technical support.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

<http://www.trendmicro.com/en/purchase/license/overview.htm>

Trend Micro, the Trend Micro t-ball logo, TrendLabs, Damage Cleanup Services, OfficeScan, PC-cillin, and ScanMail are trademarks of Trend Micro Incorporated and are registered in certain jurisdictions. All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright © 1998-2007 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. CSEM33116/70305

Release Date: March 2007

Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698; and 6,119,165

The Administrator's Guide for Trend Micro Client Server and Client Server Messaging Security for SMB is intended to introduce the main features of the software and installation instructions for your production environment. You should read it prior to installing or using the software.

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

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

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

Contents

Preface

How This Book is Organized	ii
Using Trend Micro Client Server Security for SMB Documentation ..	iii

Chapter 1: Introducing Trend Micro Client Server Security for Small and Medium Businesses

Product Overview	1-1
What's New in Client Server Security 3.6	1-3
What You Can Do with Client Server Security	1-3
Analyze Your Network's Protection	1-3
Enforce Antivirus Policies	1-4
Protect Clients and Servers from Spyware/Grayware	1-4
Update Your Protection	1-4
Perform Scans from One Location	1-4
Quarantine Infected Files	1-5
Control Outbreaks on the Network	1-5
Manage Client Server Security Groups	1-5
Protect Clients from Hacker Attacks with Personal Firewall	1-5
Protect POP3 Mail Messages	1-6
Benefits and Capabilities	1-6
Single-Console Operation	1-6
Outbreak Defense	1-6
Spyware/Grayware Approved List	1-7
Secure Web Console Communication	1-7

Chapter 2: Client Server Security Components

Overview of Client Server Security Protection	2-2
Trend Micro Security Dashboard for SMB	2-3
Trend Micro Security Server	2-4
Trend Micro Client/Server Security Agent	2-4
Client Server Security Updateable Components	2-5
About the Trend Micro Scan Engine	2-6
Scan Engine Updates	2-7

About the Virus Pattern File	2-8
About the Virus Cleanup Engine	2-8
About the Virus Cleanup Pattern	2-9
About the Common Firewall Driver	2-9
About the Network Virus Pattern File	2-9
About the Vulnerability Pattern File	2-9
About Hot Fixes, Patches, and Service Packs	2-10

Chapter 3: Planning for Installation of Client Server Security

Overview of Installation and Deployment	3-2
Phase 1: Initial Planning	3-2
Phase 2: Trend Micro Security Server Installation	3-2
Phase 3: Client/Server Security Agent Installation	3-2
Phase 4: Client Server Security Configuration	3-3
Phase 1: Initial Planning	3-3
Client Server Security Minimum Requirements	3-4
Other Requirements	3-5
Other Installation Considerations	3-6
Server Performance	3-6
Location of the Trend Micro Security Server	3-6
Number of Clients	3-7
Network Traffic Considerations	3-7
Network Traffic During Pattern File Updates	3-8
Using Update Agents to Reduce Network Bandwidth	
Consumption During Updates	3-8
Deciding on a Dedicated Server	3-9
Location of the Program Files	3-9
Number of Groups	3-9

Chapter 4: Client Server Security Installation Overview

Phase 2: Installing Client Server Security	4-2
Preparing for the Client Server Security Installation	4-2
Choosing Your Edition	4-2
Third Party Antivirus Applications	4-3
Known Compatibility Issues	4-3
Full Version and Trial Version	4-4
The Registration Key and Activation Codes	4-4

Information to Prepare Before Performing the Installation	4-5
Understanding Client Server Security Ports	4-6
Trend Micro Security Server Prescan	4-7
Actions for Prescan Detections	4-7
Other Installation Notes	4-7
Installing Client Server Security	4-8
Performing a Custom Installation	4-9
Part 1 – Pre-configuration Tasks	4-9
Part 2 – Configuring the Security Server and Security	
Dashboard Settings	4-14
Part 3 – Configuring the Client Security Agents	4-25
Performing a Typical Installation	4-28
Performing a Silent Installation	4-29
Upgrading Client Server Security	4-30
Upgrading from a Previous Version	4-30
Upgrading from an Evaluation Version	4-31
Verifying the Trend Micro Security Server Installation or Upgrade	4-32
Uninstalling the Trend Micro Security Server	4-33

Chapter 5: Installing the Trend Micro Client/Server Security Agent

Choosing an Installation Method	5-2
Installing, Upgrading, or Migrating Client/Server Security Agent	5-4
Performing a Fresh Install	5-4
Installing from the Internal Web Page	5-4
Installing with Login Script Setup	5-5
Installing with Windows 2000/Server 2003 Scripts	5-7
Installing with Client Packager	5-8
Sending the Package via Email	5-11
Installing with an MSI File	5-12
Installing with Windows Remote Install	5-12
Enabling CSA Remote Install on Windows Vista Clients	5-13
Installing with Vulnerability Scanner	5-14
Upgrading the Client/Server Security Agent	5-16
Migrating from Trend Micro Anti-Spyware	5-16
Migrating from Third-party Antivirus Applications	5-17
Automatic Client Migration	5-17
Verifying the Client Installation, Upgrade, or Migration	5-22

Using Vulnerability Scanner to Verify the Client Installation	5-22
Testing the Client Installation with the EICAR Test Script	5-24
Removing the Client Using its Uninstallation Program	5-25

Chapter 6: The Trend Micro Security Dashboard for SMB

Exploring the Security Dashboard	6-2
Getting Around the Security Dashboard	6-3

Chapter 7: Configuring Desktop and Server Groups

Configurable Options for Desktop and Server Groups	7-2
Configuring Real-time Scan	7-2
Excluding Files and Folders from Scans	7-7
Using the Personal Firewall	7-8
Personal Firewall Features	7-9
Personal Firewall Defaults for Simple Mode	7-9
Traffic Filtering	7-10
Intrusion Detection System	7-11
Exceptions	7-11
Configuring Exceptions: An Example	7-12
Configuring Personal Firewall – Simple Mode	7-12
Configuring the Personal Firewall - Advanced Mode	7-13
Disabling the Firewall	7-15
Using Desktop Privileges	7-16
Using Quarantine	7-19

Chapter 8: Using Outbreak Defense

The Outbreak Defense Strategy	8-2
Current Status	8-2
Threat Prevention	8-3
Threat Protection	8-5
Threat Cleanup	8-6
Potential Threat	8-8
Settings	8-8
Outbreak Defense	8-9
Using Exception	8-9
Using Scheduled Policy Download Settings	8-9
Vulnerability Assessment	8-10

Chapter 9: Manual and Scheduled Scans

Manual and Scheduled Scans	9-2
Scanning Desktops and Servers for Viruses, Spyware, and Other Malware Threats	9-2

Chapter 10: Updating Components

Choosing an Update Source	10-2
Updating the Components	10-3
Updating the Trend Micro Security Server	10-4
Manual and Scheduled Updates	10-4
Manual Updates	10-4
Scheduled Updates	10-4
Setting the Update Source for the Trend Micro Security Server	10-6
Default Update Times	10-7
Using Update Agents	10-8
Rolling Back Components	10-10

Chapter 11: Viewing and Interpreting Logs

Viewing and Interpreting Logs	11-2
Management Console Event Logs	11-2
Desktop/Server Logs	11-2
Using Log Query	11-3
Creating One-time Reports	11-5
Deleting One-time Reports	11-6
Scheduling Reports	11-6
Deleting Scheduled Reports	11-7
Editing Scheduled Reports	11-8
Maintaining Logs and Reports	11-9
Maintenance - Reports	11-9
Maintenance - Logs	11-10

Chapter 12: Working with Notifications

Configuring Event Notifications	12-2
Event Types	12-2
Notification Method Settings	12-4

Chapter 13: Configuring Global Settings

Internet Proxy Options	13-1
SMTP Server Options	13-2
Desktop/Server Options	13-3
General Scan Settings	13-5
Virus Scan Settings	13-5
Spyware/Grayware Scan Settings	13-6
Alert Settings	13-6
Approved List for Network Virus Scanning	13-6
Watchdog Settings	13-6
Agent Uninstallation	13-7
Agent Unloading	13-7
System Options	13-7
Removing Inactive Desktops/Servers	13-8
Verifying Client-Server Connectivity	13-9
Maintaining the Quarantine Folder	13-10

Chapter 14: Using Administrative and Client Tools

Tool Types	14-1
Summary of Tools	14-2
Administrative Tools	14-2
Login Script Setup	14-3
Vulnerability Scanner	14-3
Other Settings	14-6
Client Tools	14-7
Client Packager	14-8
Restore Encrypted Virus	14-8
Touch Tool	14-10
Client Mover	14-11

Chapter 15: Performing Additional Administrative Tasks

Changing the Security Dashboard Password	15-2
Viewing Product License Details	15-3
Participating in the World Virus Tracking Program	15-3

Chapter 16: Understanding the Threats

What Do the Terms Mean?	16-2
-------------------------------	------

Viruses	16-2
Network Viruses	16-3
Trojans	16-4
Bots	16-4
Packers	16-4
Worms	16-4
About ActiveX	16-5
About Mass-Mailing Attacks	16-5
About Macro Viruses	16-6
Guarding Against Malicious or Potentially Malicious Applications	16-6

Chapter 17: FAQs, Troubleshooting and Technical Support

Frequently Asked Questions (FAQs)	17-2
Registration	17-2
Installation, Upgrade, and Compatibility	17-2
Configuring Settings	17-3
Documentation	17-3
Troubleshooting	17-4
Restoring Program Settings after Rollback or Reinstallation	17-4
Some Client Server Security Components are not Installed	17-5
Unable to Access the Web Console	17-5
Browser Cache	17-6
SSL Certificate	17-6
Virtual Directory Settings	17-6
Incorrect Number of Clients on the Security Dashboard	17-7
Unsuccessful Installation from Web Page or Remote Install	17-7
Client Icon Does Not Appear on Security Dashboard after Installation	17-8
Issues During Migration from Third-party Antivirus Software ..	17-8
Client Migration	17-8
The Trend Micro Security Information Center	17-10
Known Issues	17-11
Contacting Technical Support	17-12
Speeding Up Your Support Call	17-12
The Trend Micro Knowledge Base	17-12
Sending Suspicious Files to Trend Micro	17-13
About TrendLabs	17-13

Appendix A: System Checklists

Server Address Checklist	A-1
Ports Checklist	A-3

Appendix B: Trend Micro Services

Trend Micro Outbreak Prevention Policy	B-1
Trend Micro Damage Cleanup Services	B-2
The Damage Cleanup Services Solution	B-2
Vulnerability Assessment	B-3
Trend Micro IntelliScan	B-3
Trend Micro ActiveAction	B-4
Trend Micro IntelliTrap	B-4
True File Type	B-4
About ActiveAction	B-5

Appendix C: Planning a Pilot Deployment

Choosing a Pilot Site	C-1
Creating a Rollback Plan	C-1
Deploying Your Pilot	C-2
Evaluating Your Pilot Deployment	C-2

Appendix D: Trend Micro Product Exclusion List

Appendix E: Client Side Information

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

Appendix F: Spyware Types

Appendix G: Glossary of Terms

Preface

Welcome to the *Trend Micro Client Server Security for Small and Medium Businesses Version 3.6 Administrator's Guide*. This book contains information about the tasks you need to do to install and configure Client Server Security. This book is intended for novice and experienced users of Client Server Security who want to quickly configure, administer, and use the product.

How This Book is Organized

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

- **Section 1** – The first section of this document consists of three chapters, 1-3, that introduce the product and address pre-installation and planning.
- **Section 2** – The second section consists of two chapters, 4-5, and covers product and component installation.
- **Section 3** – The third section, chapters 6-15, provides high-level descriptions of the Security Dashboard and information about accomplishing configuration related tasks.
- **Section 4** – The fourth section contains two chapters, 16-17, that provide support related information such as FAQ, how to finding help, reference information.
- **Section 5** – The fifth section contains 5 Appendices that provide additional information and resources.

Using Trend Micro Client Server Security for SMB Documentation

The documentation set for Trend Micro Client Server Security for SMB includes the following:

- **Administrator's Guide** – This guide helps you configure Client/Server Security Agent options. The latest version of the *Administrator's Guide* is available in electronic form at the following location:
<http://www.trendmicro.com/download/>
- **Getting Started Guide** – This guide helps you plan for and install the Trend Micro Security Server program, modify important default client settings, and roll out your clients. The latest version of the *Getting Started Guide* is available in electronic form at the following location:
<http://www.trendmicro.com/download/>
- **Online help** – The purpose of online help is to provide descriptions for performing the main tasks, usage advice, and field-specific information, such as valid parameter ranges and optimal values. Online help is accessible from the Trend Micro Security Dashboard for SMB .
- **Readme file** – The Readme file contains late-breaking product information not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and product release history.
- **Knowledge Base** – The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site:

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

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

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

Introducing Trend Micro Client Server Security for Small and Medium Businesses

This chapter provides an overview of Client Server Security's key features and capabilities.

The topics discussed in this chapter include:

- *Product Overview* on page 1-1
- *What's New in Client Server Security 3.6* on page 1-3
- *What You Can Do with Client Server Security* on page 1-3
- *Benefits and Capabilities* on page 1-6

Product Overview

Designed to suit the needs of small- to medium-sized business IT networks, Trend Micro Client Server Security for SMB provides network-wide desktop and server protection.

Network-wide desktop and server protection helps shield servers and computers on the network from virus and spyware/grayware threats. Client Server Security keeps

computers on your network up-to-date with the latest pattern files through centralized management and automatic updates of client installations.

Seamless integration with Microsoft™ Windows™ and Microsoft Exchange Server™ makes Client Server Security a powerful, multi-layered defense against viruses, spyware, and other malicious code. Centralized management tools and intelligent malicious code scanning offers excellent antivirus and content security in a scalable high-performance software architecture.

This manual describes how to install, configure, maintain, and troubleshoot Client Server Security. You can view electronic copies of product manuals in PDF form on the Trend Micro Small and Medium Business Solution CD. PDF files are located on the CD in the documents folder.

```
{CD-ROM drive}\Documentation
```

Replace {CD-ROM drive} with the drive letter of the CD-ROM drive on your computer.

What's New in Client Server Security 3.6

This version of Client Server Security inherits all the features of previous versions and provides the following new feature:

- **Windows Vista Support**—Client Server Messaging Security Agent clients can now be installed on Windows Vista (32-bit and 64-bit) clients. Refer to Table E-3 for a comparison of the CSA features on different platforms.

What You Can Do with Client Server Security

Perform key administrative tasks using the Security Dashboard:

- *Analyze Your Network's Protection* on page 1-3
- *Enforce Antivirus Policies* on page 1-4
- *Protect Clients and Servers from Spyware/Grayware* on page 1-4
- *Update Your Protection* on page 1-4
- *Perform Scans from One Location* on page 1-4
- *Quarantine Infected Files* on page 1-5
- *Control Outbreaks on the Network* on page 1-5
- *Manage Client Server Security Groups* on page 1-5
- *Protect Clients from Hacker Attacks with Personal Firewall* on page 1-5
- *Protect POP3 Mail Messages* on page 1-6

Analyze Your Network's Protection

Client Server Security can generate various types of logs, including virus logs, system event logs, and update logs. Use these logs to verify update deployment, check client-server communication, and determine which computers are vulnerable to infection.

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

Enforce Antivirus Policies

Client Server Security provides three types of scans: Scheduled Scan, Manual Scan, and Real-time Scan. Enforce your organization's antivirus policies by configuring these three types of scans. Specify the types of files to scan and the action to take when Client Server Security finds a virus.

To apply uniform scan settings to all clients, choose not to grant privileges to clients and lock the client program with a password to prevent users from removing or turning it off.

Protect Clients and Servers from Spyware/Grayware

In addition to protecting against viruses, Client Server Security also checks for and removes any spyware installed on clients and servers. As with antivirus scanning, three types of anti-spyware scans are available – Scheduled Scan, Manual Scan, and Real-time Scan.

Each scan type provides the option to run either a full scan (all files and registries) or a quick scan (registry only). Available scan actions for spyware include Clean (remove) and Pass (record to log only).

Update Your Protection

Virus writers create new viruses and release them everyday. To ensure that you stay protected against the latest threats, you must periodically update the Client Server Security components. Trend Micro usually releases new virus pattern files on a daily basis.

Perform Scans from One Location

The Security Dashboard provides the option of performing Scan Now (Manual Scan) and configuring scheduled scans on clients to run during off-peak hours when client CPU usage is low.

Quarantine Infected Files

You can specify a quarantine folder to control live viruses and infected files. The Trend Micro Security Server then automatically forwards infected files to the quarantine folder.

Control Outbreaks on the Network

Enabling Outbreak Defense and setting up outbreak notifications helps you to respond quickly to outbreaks that may be developing.

Outbreak Defense helps stop outbreaks from overwhelming your network by blocking shared folders and vulnerable ports on clients and by denying write access to folders. Download the latest pattern file and then perform Scan Now on all clients to remove any existing threats.

Manage Client Server Security Groups

A group in Client Server Security is a cluster of clients that share the same configuration and run the same tasks. A Client Server Security group is different from a Windows domain. There can be several Client Server Security groups in any given Windows domain.

Group clients into Client Server Security groups to simultaneously apply the same configuration to all group members.

Protect Clients from Hacker Attacks with Personal Firewall

Help protect clients running Windows 2000/XP/Server 2003 from hacker attacks and network viruses by creating a barrier between the client machine and the network. Personal Firewall allows you to block or allow certain types of network traffic. Additionally, Personal Firewall will identify patterns in network packets that may indicate an attack on clients.

Protect POP3 Mail Messages

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

Benefits and Capabilities

Trend Micro Client Server Security for SMB brings many benefits to your organization by providing a comprehensive yet user-friendly method of managing your antivirus policies. The following is a summary of the advantages you can obtain.

Single-Console Operation

The Trend Micro Security Server allows you to manage your entire anti-virus system through a single Web console. The Trend Micro Security Dashboard for SMB is installed when you install the Trend Micro Security Server and uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

Outbreak Defense

Use Outbreak Defense to take preemptive steps to secure your network. Outbreak Defense first informs you of the latest threats, and then takes action to shield your network and clients from the threat. While Outbreak Defense is protecting your network and clients, TrendLabs is busy creating a solution to the threat. As soon as TrendLabs finds a solution, they release updated components. The Security Server then downloads and deploys the updated components to clients. For the last step, Outbreak Defense cleans up any virus remnants, and repairs files and directories that have been damaged by the threat.

Using Outbreak Defense, you can take the following actions in the event of an outbreak:

- Block ports to help prevent viruses from infecting files on the network
- *Write-protect* certain files and directories

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.

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

If you want to run Hotbar or any other application that Client Server Security classifies as spyware/grayware, you need to add it to the spyware/grayware approved list.

By preventing potentially risky applications from running and by giving you full control over the spyware/grayware approved list, Client Server Security helps ensure that only the applications you approve run on clients and servers.

Secure Web Console Communication

Client Server Security provides secure communications between the Trend Micro Security Server and the Security Dashboard through Secure Socket Layer (SSL) technology.

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

Client Server Security Components

This chapter provides a brief overview of Client Server Security protection, and describes the components that Client Server Security uses to carry out the protection.

The topics discussed in this chapter include:

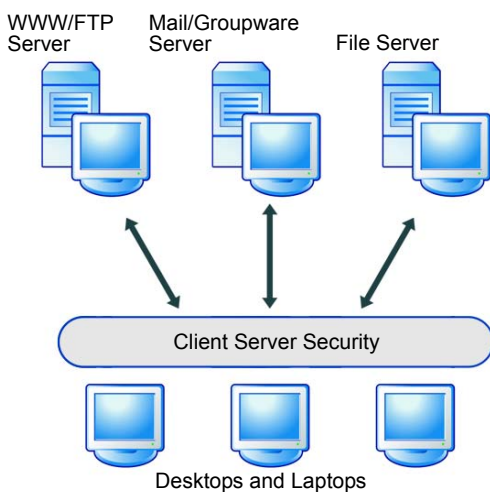
- *Overview of Client Server Security Protection* on page 2-2
- *Trend Micro Security Dashboard for SMB* on page 2-3
- *Trend Micro Security Server* on page 2-4
- *Trend Micro Client/Server Security Agent* on page 2-4
- *Client Server Security Updateable Components* on page 2-5

Overview of Client Server Security Protection

Trend Micro Client Server Security is a centrally managed antivirus solution for desktops, notebook computers, and servers. Client Server Security helps protect your organization's Windows™ Vista/2000/XP/Server 2003 computers from a wide range of threats and potential nuisances, such as file viruses, spyware/grayware, macro viruses, malicious Java™ applets and ActiveX™ controls.

The antivirus function of Client Server Security is provided through the client, which reports to and gets updates from the server. The Trend Micro Security Dashboard for SMB allows you to configure, monitor, and update clients.

FIGURE 2-1. Client Server Security Protection



Client Server Security includes the following:

- Trend Micro Security Dashboard for SMB manages all clients from a single location.
- Trend Micro Security Server, which hosts the Trend Micro Security Dashboard for SMB, downloads updates from the Trend Micro ActiveUpdate server, collects and stores logs, and helps control virus outbreaks.
- Trend Micro Client/Server Security Agent, which protects your Windows Vista/2000/XP/Server 2003 computers from viruses, spyware, Trojans, and other threats

Trend Micro Security Dashboard for SMB

The Trend Micro Security Dashboard for SMB is the central point for monitoring Client Server Security across the entire network, as well as for configuring Trend Micro Security Server and client settings.

Client Server Security gives you complete control over desktop, notebook, and server antivirus settings. Use the Security Dashboard to do the following:

- Deploy the Client/Server Security Agent program to desktops, notebooks, and servers.
- Cluster desktops, notebooks, and servers into logical groups for simultaneous configuration and management.
- Set antivirus and anti-spyware scan configurations and start Manual Scan on a single group or on multiple groups.
- Receive notifications and view log reports for virus activities.
- When spyware or viruses are detected on clients, receive notifications and send virus outbreak alerts via email, SNMP Trap, or Windows Event Log.
- Control outbreaks by configuring and enabling Outbreak Prevention.

The Security Dashboard is installed when you install Trend Micro Security Server. The Security Dashboard uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

Open the Security Dashboard from any computer that has a Web browser that meets the minimum requirements.

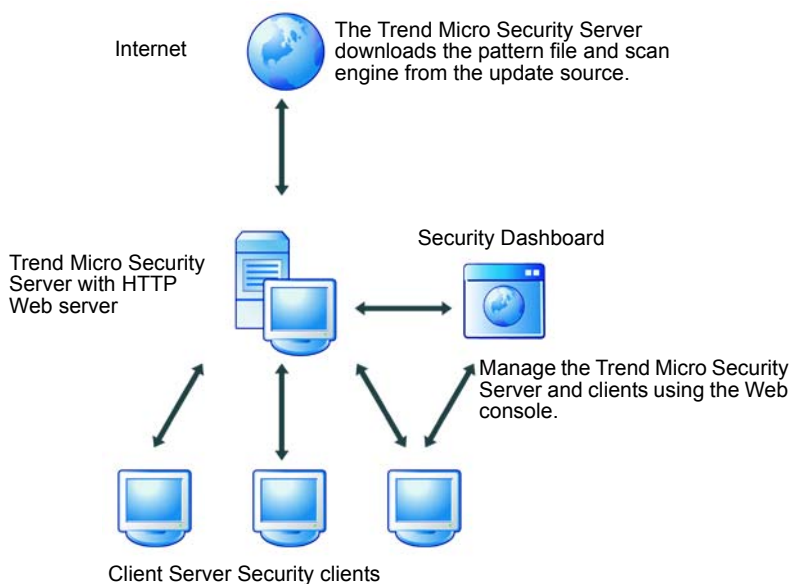
Trend Micro Security Server

The Trend Micro Security Server is the central repository for all client configurations, virus logs, and client software and updates.

The Trend Micro Security Server performs these important functions:

- It installs, monitors, and manages clients on the network
- It downloads virus pattern files, spyware pattern files, scan engines, and program updates from the Trend Micro update server, and then distributes them to clients

FIGURE 2-2. How Client-Server Communication via HTTP Works



Trend Micro Client/Server Security Agent

Protect Windows computers from viruses and spyware by installing the Client/Server Security Agent on each desktop, notebook, and server. The Client/Server Security Agent provides three methods of scanning: Real-time Scan, Scheduled Scan, Manual Scan.

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

Configure scan settings on clients from the Trend Micro Security Dashboard for SMB . To enforce uniform desktop protection across the network, choose not to grant the clients privileges to modify the scan settings or to remove the client program.

Client Server Security Updateable Components

Client Server Security uses the following components to scan for, identify, and perform damage cleanup tasks to help protect and clean clients:

- **Virus pattern file** – A file that helps Client Server Security identify virus signatures– unique patterns of bits and bytes that signal the presence of a virus
- **Virus scan engine 32-bit** – The engine Client Server Security uses to scan for viruses.
- **Virus scan engine 64-bit** – The engine Client Server Security uses to scan for viruses
- **Virus cleanup template** – Used by the virus cleanup engine, this template helps identify viruses, Trojans and Trojan processes
- **Virus cleanup engine 32-bit** – The engine Damage Cleanup Services™ uses to scan for and remove from memory viruses, Trojans and Trojan processes, and other malware.
- **IntelliTrap exception pattern** – The pattern that the Virus Scan Engines use to identify exceptions to items listed in the IntelliTrap pattern.
- **IntelliTrap pattern** – The pattern that the Virus Scan Engines use to detect malicious code such as bots in compressed files.
- **Vulnerability pattern** – A file that helps Client Server Security identify vulnerabilities on client machines
- **Common firewall pattern** – Like the virus pattern file, this file helps Client Server Security identify virus signatures.
- **Common firewall engine 32-bit** – The driver the Personal Firewall uses with the network virus pattern file to scan client machines for network viruses

- **Spyware Pattern** – Contains known spyware signatures and used by the spyware scan engines (both 32-bit and 64-bit) to detect spyware on clients and servers for manual and scheduled scans
- **Spyware Active-monitoring Pattern** – Similar to spyware pattern, but is used by the scan engine for real-time anti-spyware scanning
- **Spyware Scan Engine (32-bit)** – A separate scan engine that scans for, detects, and removes spyware from infected clients and servers running on i386 (32-bit) operating systems (for example, Windows Vista, Windows 2000, and Windows XP)
- **Spyware Scan Engine (64-bit)** – Similar to the spyware scan engine for 32-bit systems, this scan engine scans for, detects, and removes spyware on x64 (64-bit) operating systems (for example, Windows Vista x64, Windows XP Professional x64 Edition, Windows 2003 x64 Edition)
- **Anti-Rootkit Driver (32-bit)** – A module required by the scan engine to detect rootkits
- **Hot fixes and security patches** – Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the Trend Micro Security Server and/or client program

About the Trend Micro Scan Engine

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

- **Actively circulating** – Threats that are actively circulating on the Internet
- **Known and controlled** – Controlled viruses not in circulation, but that are developed and used for research

Rather than scan every byte of every file, the engine and pattern file work together to identify not only tell-tale characteristics of the virus code, but the precise location within a file where the virus would hide. If Client Server Security detects a virus, it can remove it and restore the integrity of the file.

The scan engine includes an automatic clean-up routine for old virus pattern files (to help manage disk space), as well as incremental pattern updates (to help manage bandwidth).

In addition, the scan engine is able to decrypt all major encryption formats (including MIME and BinHex). It also recognizes and scans common compression formats, including Zip, Arj, and Cab. Client Server Security also allows you to determine how many layers of compression to scan (up to a maximum of six), for compressed files contained within a file.

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

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

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

Scan Engine Updates

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

- New scanning and detection technologies are incorporated into the software
- A new, potentially harmful virus is discovered that the scan engine cannot handle
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

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

<http://www.trendmicro.com>

About the Virus Pattern File

The Trend Micro scan engine uses an external data file, called the virus pattern file. It contains information that helps Client Server Security identify the latest viruses and other Internet threats such as Trojan horses, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly threat is discovered.

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

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

You can download virus pattern files from the following Web site, where you can also find the current version, release date, and a list of all the new virus definitions included in the file:

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

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique “signature” or string of telltale characters that distinguish it from any other code, the virus experts at TrendLabs™ capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When the engine detects a match, a virus has been detected and an email notification is sent to the system administrator.

About the Virus Cleanup Engine

Damage Cleanup Services (DCS) makes use of a scanning and cleanup tool called the Virus Cleanup Engine (VCE) to find and repair damage caused by viruses and other Internet threats. The Virus Cleanup Engine can find and clean viruses, Trojans, and other malware. The VCE is essentially a software agent that makes use of a database to find targeted machines and evaluate whether viruses or other Internet

threats have affected them. VCE resides on a single machine and deploys to the targeted client machines on the network at the time of scanning.

The Virus Cleanup Engine uses damage cleanup templates that contain information that VCE uses to restore damage caused by the latest known viruses, malware, or other Internet threats. DCS regularly updates these templates. When you install DCS, you are installing the version of the Virus Cleanup Engine that was current as of the release of this product. TrendLabs updates the Virus Cleanup Pattern frequently, therefore, Trend Micro recommends that you update your components immediately after you have installed and activated Damage Cleanup Services.

About the Virus Cleanup Pattern

The Virus Cleanup Engine uses the Virus Cleanup Pattern to identify Trojans, network viruses, and active malware.

About the Common Firewall Driver

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

About the Network Virus Pattern File

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

About the Vulnerability Pattern File

Client Server Security deploys the Vulnerability Pattern file after updating components. The Vulnerability Pattern file is used in the **Outbreak Defense > Potential Threat** screen when the Scan for Vulnerability Now tool is used, or when scheduled Vulnerability Assessment is triggered, or whenever a new Vulnerability Pattern file is downloaded. As soon as the Trend Micro Security Server completes

downloading a new Vulnerability Pattern file, Client Server Security starts to scan clients for vulnerabilities.

About Hot Fixes, Patches, and Service Packs

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

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

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

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

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

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

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

Note: All releases include a readme file with the information you need to install, deploy, and configure your product. Read the readme file carefully before installing the hot fix, patch, or service pack file(s).

Planning for Installation of Client Server Security

This chapter outlines the phases necessary for the successful installation and deployment of Trend Micro Client Server Security for SMB and provides instructions for the first phase: planning. Read this chapter carefully before performing installation.

The topics discussed in this chapter include:

- *Client Server Security Minimum Requirements* on page 3-4
- *Location of the Trend Micro Security Server* on page 3-6
- *Number of Clients* on page 3-7
- *Network Traffic Considerations* on page 3-7
- *Using Update Agents to Reduce Network Bandwidth Consumption During Updates* on page 3-8
- *Location of the Program Files* on page 3-9
- *Number of Groups* on page 3-9

Overview of Installation and Deployment

This section outlines the phases for Client Server Security installation and deployment. Each phase has corresponding sections that discuss in detail the tasks that you need to perform.

Phase 1: Initial Planning

During this phase, plan how to deploy Trend Micro Client Server Security for SMB by verifying and considering the following information:

- *Client Server Security Minimum Requirements* on page 3-4
- *Location of the Trend Micro Security Server* on page 3-6
- *Number of Clients* on page 3-7
- *Network Traffic Considerations* on page 3-7
- *Location of the Program Files* on page 3-9
- *Number of Groups* on page 3-9

Phase 2: Trend Micro Security Server Installation

During this phase, use the master installer to install the Trend Micro Security Server. Complete this phase by performing the following tasks:

- *Preparing for the Client Server Security Installation* on page 4-2
- *Installing Client Server Security* on page 4-8
- *Verifying the Trend Micro Security Server Installation or Upgrade* on page 4-32

Phase 3: Client/Server Security Agent Installation

During this phase, complete your installation and deployment by rolling out the Client/Server Security Agent to your desktops and servers. Complete this phase by performing the following tasks:

- *Choosing an Installation Method* on page 5-2
- *Installing, Upgrading, or Migrating Client/Server Security Agent* on page 5-4
- *Verifying the Client Installation, Upgrade, or Migration* on page 5-22

- *Testing the Client Installation with the EICAR Test Script* on page 5-24

Phase 4: Client Server Security Configuration

After installing the Client/Server Security Agent to your clients, modify the default settings if necessary to ensure that the settings are in line with your antivirus and security initiatives:

- *Configuring Desktop and Server Groups* on page 7-1
- *Configuring Global Settings* on page 13-1

Phase 1: Initial Planning

The steps in this phase help you develop a plan for Client Server Security installation and deployment. Trend Micro highly recommends creating an installation and deployment plan before performing installation. Creating an installation and deployment plan will help ensure that you incorporate Client Server Security's capabilities into your existing antivirus and network protection plan.

Client Server Security Minimum Requirements

The computer(s) running the Trend Micro Security Server program and any computer accessing the Trend Micro Security Dashboard for SMB need to meet the minimum requirements listed in this section.

TABLE 3-1. Component Minimum System Requirements

Client Server Security - Components	Minimum System Requirements				Other Requirements
	CPU	RAM	Disk Space	OS	
Trend Micro Security Server	733MHz	512MB	1GB	Win 2000 SP2 Win XP SP1 Win 2003 (R2) SBS2000 SBS2003 (R2)	Security Server: IE5.5 Web Server: IIS5.0 IIS5.1 IIS6.0 Apache2.0.54 Web Console: IE5.5 (Hi-color display adaptor w/1024x768 resolution)
Client/Server Security Agent	300MHz	128MB	200MB	Win Vista Win Vista x64 Win 2000 SP2 Win XP Win XP Pro x64 Win 2003 (R2) Win 2003 x64 (R2) SBS 2000 (R2) SBS 2003 (R2)	Monitor: 800x600 resolution

WARNING! *You have the option of installing Apache Web server when you install the Trend Micro Security Server. By default, the administrator account is the only account created on the Apache Web server. Trend Micro recommends creating another account from which to run the Web server; otherwise a hacker may be able to take control of the Apache server and compromise the Trend Micro Security Server.*

Before installing the Apache Web server, refer to the Apache Web site for the latest information on upgrades, patches, and security issues:

<http://www.apache.org>.

Note: If using Remote install to install the Client/Server Security Agent on Windows Vista/XP clients, you must disable **Simple File Sharing** unless they are part of a domain (see your Windows documentation for instructions).

Other Requirements

- Administrator or Domain Administrator access on the computer hosting the Security Server
 - File and printer sharing for Microsoft Networks installed
 - Transmission Control Protocol/Internet Protocol (TCP/IP) support installed
-

Note: If Microsoft ISA Server or a proxy product is installed on the network, you need to enable the HTTP port (80 or 8080) and SSL port (443 or 4343) to enable access to the Security Dashboard and to ensure that client-server communication can be established.

Other Installation Considerations

Server Performance

Ideally, the computer on which the Trend Micro Security Server is installed would have the following:

- Single 2.8~3.2 GHz processor
- 500 MB of memory

Location of the Trend Micro Security Server

Client Server Security is flexible enough to accommodate a variety of network environments. For example, you can position a firewall between the Trend Micro Security Server and clients running the Client/Server Security Agent, or position both the Trend Micro Security Server and all Client/Server Security Agent clients behind a single network firewall.

Ideally, the Security Server should be located behind a firewall and there should not be a firewall between the clients and the security server.

If managing more than one site, having a security server at the main site as well as at each managed site will reduce bandwidth usage between the main site and managed sites, and speed up pattern deployment rates.

If client computers have the Windows XP Firewall enabled, Client Server Security will automatically add it to the Exception list.

Note: If a firewall is located between the Trend Micro Security Server and its clients, you must configure the firewall to allow traffic between the client listening port and Trend Micro Security Server's listening port (see *Understanding Client Server Security Ports* on page 4-6 for more information on the types of ports the client and the Trend Micro Security Server use to communicate)

Number of Clients

A client is a computer that has the Client/Server Security Agent software installed on it. Clients can be desktops, servers (even Exchange servers), and notebook computers, including those that belong to users who telecommute or connect to the corporate network from their homes.

If you have a heterogeneous client base (that is, if your network has different Windows operating systems, such as Windows Vista/2000/XP/Server 2003), identify how many clients are using a specific Windows version. Use this information to decide which client deployment method will work best in your environment.

Note: A single Trend Micro Security Server can manage up to **2500** clients. If you have more than this amount, Trend Micro suggests installing more than one Trend Micro Security Server.

Network Traffic Considerations

When planning for deployment, consider the network traffic that Client Server Security will generate. Client Server Security generates network traffic when the Trend Micro Security Server and clients communicate with each other.

The Trend Micro Security Server generates traffic when it does the following:

- Connects to the Trend Micro ActiveUpdate server to check for and download updated components
- Notifies clients to download updated components
- Notifies clients about configuration changes

The client generates traffic when it does the following:

- Starts up
- Performs scheduled update
- Switches between roaming mode and normal mode
- Performs Update Now
- Generates a Virus Log

Network Traffic During Pattern File Updates

Significant network traffic is generated whenever TrendLabs releases an updated version of any of the following items:

- Virus pattern, Virus scan engine 32-bit, Virus scan engine 64-bit
- IntelliTrap pattern, IntelliTrap exception pattern
- Virus cleanup template, Virus cleanup engine 32-bit
- Spyware pattern, spyware active-monitoring pattern, anti-rootkit driver (for 32-bit systems only), and spyware scan engine
- Anti-spam pattern, Anti-spam engine
- Vulnerability pattern
- Common Firewall pattern, Common Firewall driver 32-bit

To reduce network traffic generated during pattern file updates, Client Server Security uses a method called incremental update. Instead of downloading the full updated pattern file every time, the Trend Micro Security Server only downloads the new patterns that have been added since the last release. The Trend Micro Security Server merges the new patterns with the old pattern file.

Regularly updated clients only have to download the incremental pattern, which is approximately 5KB to 200KB. The full pattern is approximately 13MB when compressed and 20MB to 30MB when uncompressed and takes substantially longer to download.

Trend Micro releases new pattern files daily. However, if a particularly damaging virus is actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available.

Using Update Agents to Reduce Network Bandwidth Consumption During Updates

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

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

Deciding on a Dedicated Server

When selecting a server that will host Client Server Security, consider the following:

- How much CPU load is the server carrying?
- What other functions does the server perform?

If you are installing Client Server Security on a server that has other uses (for example, application server), Trend Micro recommends that you install on a server that is not running mission-critical or resource-intensive applications.

Location of the Program Files

During the Trend Micro Security Server installation, specify where to install the program files on the clients. Either accept the default client installation path or modify it. Trend Micro recommends that you use the default settings, unless you have a compelling reason (such as insufficient disk space) to change them.

The default client installation path is:

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

Number of Groups

A group in Client Server Security is a cluster of clients that share the same configuration and run the same tasks. By clustering your clients into groups, you can simultaneously configure, manage, and apply the same configuration to all group members.

A Client Server Security group is different from a Windows domain. There can be several Client Server Security groups in one Windows domain.

For ease of management, plan how many Client Server Security groups to create. You can group clients based on the departments they belong to or the functions they

perform. Alternatively, you can group clients that are at a greater risk of infection and apply a more secure configuration to all of them.

Client Server Security Installation Overview

This chapter explains the steps necessary for the next phase: Client Server Security installation or upgrade. It also provides information on uninstalling the Trend Micro Security Server program.

The topics discussed in this chapter include:

- *Preparing for the Client Server Security Installation* on page 4-2
- *Installing Client Server Security* on page 4-8
- *Performing a Custom Installation* on page 4-9
- *Performing a Typical Installation* on page 4-28
- *Performing a Silent Installation* on page 4-29
- *Upgrading Client Server Security* on page 4-30
- *Verifying the Trend Micro Security Server Installation or Upgrade* on page 4-32
- *Uninstalling the Trend Micro Security Server* on page 4-33

Phase 2: Installing Client Server Security

The steps in this phase help you prepare for Client Server Security installation and outline how to perform a fresh install or an upgrade.

Tip: You can preserve your client settings when you upgrade to this version of Client Server Security or if you need to reinstall this version of Client Server Security. See [Upgrading from a Previous Version](#) on page 4-30 for instructions.

Preparing for the Client Server Security Installation

This section provides background information you will need to understand before performing the installation.

Choosing Your Edition

The Activation Code that you receive from Trend Micro depends on the product purchased.

The following tables list the features supported for each edition.

TABLE 4-1. Features Available by Product Types

Features	Client Server Security	Client Server Messaging Security
Component Updates	Yes	Yes
Antivirus	Yes	Yes
Firewall	Yes	Yes
Anti-spyware	Yes	Yes
Anti-spam	No	Yes
Content Filtering	No	Yes
Attachment Blocking	No	Yes

TABLE 4-2. License Status Consequences

	Fully Licensed	Evaluation (30 days)	Expired
Expiration Notification	Yes	Yes	Yes
Virus Pattern File Updates	Yes	Yes	No
Program Updates	Yes	Yes	No
Technical Support	Yes	No	No
Real-time Scanning	Yes	Yes	Yes

Note: To upgrade your edition, contact a Trend Micro sales representative.

Third Party Antivirus Applications

Trend Micro highly recommends removing third party antivirus applications from the computer on which you will install the Trend Micro Security Server. The existence of other antivirus applications on the same computer may hinder proper Trend Micro Security Server installation and performance.

Note: Client Server Security cannot uninstall the server component of any third-party antivirus product, but can uninstall the client component (see [Migrating from Third-party Antivirus Applications](#) on page 5-17 for instructions and for a list of third party applications Client Server Security can remove).

Known Compatibility Issues

This section explains compatibility issues that may arise if you install the Trend Micro Security Server on the same computer with certain other third-party applications. Always refer to the documentation of all third-party applications that are installed on the same computer on which you will install the Trend Micro Security Server.

SQL Server

You can scan SQL Server databases; however, this may decrease the performance of applications that access the databases. Trend Micro recommends excluding SQL Server databases and their backup folders from Real-time Scan. If you need to scan a database, perform a manual scan during off-peak hours to minimize the impact of the scan.

Internet Connection Firewall (ICF)

Windows XP SP2 and Windows Server 2003 provide a built-in firewall named Internet Connection Firewall (ICF). Trend Micro highly recommends removing any third-party firewall applications if you want to install Personal Firewall. However, if you want to run ICF or any other third-party firewall, add the Trend Micro Security Server listening ports to the firewall exception list (see *Understanding Client Server Security Ports* on page 4-6 for information on listening ports and see your firewall documentation for details on how to configure exception lists).

Full Version and Trial Version

You can install either a full version of Client Server Security or a free, trial version.

- **Full version** – Comes with technical support, virus pattern downloads, real-time scanning, and program updates for one year. You can renew a full version by purchasing a maintenance renewal.
- **Trial version** – Provides real-time scanning and updates for 30 days. You can upgrade from a trial version to a full version at any time.

The Registration Key and Activation Codes

Your version of Client Server Security comes with a Registration Key. During installation, Client Server Security prompts you to enter an Activation Code.

If you do not have the Activation Code(s), use the Registration Key that came with your product to register on the Trend Micro Web site and receive the Activation Code(s). The Client Server Security master installer can automatically redirect you to the Trend Micro Web site:

<http://www.trendmicro.com/support/registration.asp>

If you do not have either the Registration Key or Activation Code, you can still install the trial version. The trial version has all the same functionality as the full version, and if you upgrade within 30 days all of your settings will automatically be upgraded to the full version. To find out more information contact your Trend Micro sales representative (see *Contacting Technical Support* on page 17-12).

Note: For more information about registration, visit the Trend Micro Web site at <http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326>

Information to Prepare Before Performing the Installation

The master installer will prompt you for the following information during installation:

- **Security server details** – The domain/hostname or the IP address of the security server and the target directory where Client Server Security installs the security server files.
- **Proxy server details** – If a proxy server handles Internet traffic on your network, you must configure proxy server information (including the user name and password). This information is necessary to download the latest components from the Trend Micro update server. You can enter proxy server information during or after installation. Use the Trend Micro Security Dashboard for SMB to enter information after installation.
- **SMTP server** – If using an SMTP server to send notifications, enter the name of the SMTP server, the port number, and the recipients' email address.

Note: The installation program will automatically detect the name of the SMTP server and fill in the field if the SMTP server is on the same computer as the Security Server installation.

- **Dashboard password** – To prevent unauthorized access to the Trend Micro Security Dashboard for SMB, you can specify a password that will be required of anyone trying to open the console.

- **Client unload/uninstall password** – Set a password to prevent unauthorized unloading or removal of the Client/Server Security Agent.
- **Client software installation path** – Configure the client installation path where Client Server Security files will be copied to during client setup.
- **Account and Privileges** – You must log on with an administrator account with domain administrator privileges, or with administrator privileges on the local computer. If you do not log on with domain administrator privileges or local computer privileges, you must manually create an administrative group before proceeding with the installation.

Understanding Client Server Security Ports

Client Server Security utilizes two types of ports:

- **Server listening port (HTTP port):** used to access the Trend Micro Security Server. By default, Client Server Security uses one of the following:
 - **IIS server default Web site** – The same port number as your HTTP server's TCP port.
 - **IIS server virtual Web site** – 8059
- **Apache server** – 8059
- **Client listening port** – A randomly generated port number through which the client receives commands from the Trend Micro Security Server.

You can modify the server listening port during installation or after. You can modify the client listening port only during installation.

WARNING! *Many hacker and virus attacks use HTTP and are directed at ports 80 and/or 8080– commonly used in most organizations as the default Transmission Control Protocol (TCP) ports for HTTP communications. If your organization is currently using one of these ports as the HTTP port, Trend Micro recommends using another port number.*

Trend Micro Security Server Prescan

Before the master installer begins the installation process, it performs a prescan. This prescan includes a virus scan and Damage Cleanup Services scan to help ensure the target computer does not contain viruses, Trojans, or other potentially malicious code.

The prescan targets the most vulnerable areas of the computer, which include the following:

- the Boot area and boot directory (for boot viruses)
- the Windows folder
- the Program Files folder

Actions for Prescan Detections

If the Client Server Security setup program detects viruses, Trojans, or other potentially malicious code, you can take the following actions:

- **Clean** – Cleans an infected file by removing the virus or malicious application. Client Server Security encrypts and renames the file if the file is uncleanable.
- **Rename** – Encrypts the file and changes the file extension to .VIR, .VIR1, .VIR2... The file remains in the same location.
- **Delete** – Deletes the file.
- **Pass** – Does nothing to the file.

Tip: Trend Micro recommends cleaning or deleting infected files.

Other Installation Notes

Installing the Trend Micro Security Server does not require you to restart the computer. After completing the installation, immediately configure the Trend Micro Security Server, and then proceed to rolling out the Client/Server Security Agent program. If using an IIS Web server, the setup program automatically stops and restarts the IIS service during Web server installation.

WARNING! *Make sure that you do not install the Web server on a computer that is running applications that might lock IIS. This could prevent successful installation. See your IIS documentation for more information.*

Tip: Trend Micro highly recommends installing Client Server Security during non-peak hours to minimize the effect on your network.

Installing Client Server Security

There are three methods for installing Client Server Security:

- **Typical:** provides a simple and easy solution for installing Client Server Security using Trend Micro default values. This method is suitable for a single small business using a single Trend Micro Security Server and up to ten client desktops.
- **Custom:** provides flexibility in implementing your network security strategy. This method is suitable if you have many computers and servers, or multiple Exchange servers.
- **Silent:** performing a Silent installation creates a record file that you can use to perform identical installations on other computers or networks.

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

Tip: You can preserve your client settings when you upgrade to this version of Client Server Security or if you need to reinstall this version of the Client Server Security. See *Upgrading from a Previous Version* on page 4-30 for instructions.

Performing a Custom Installation

The Custom Installation method provides the most flexibility in implementing your network security strategy. The Custom and Typical installation processes follow a similar flow:

1. Perform pre-configuration tasks
2. Enter the settings for the Trend Micro Security Server and Security Dashboard
3. Configure the Client/Server Security Agent installation options for local and remote client computers
4. Start the installation process

Part 1 – Pre-configuration Tasks

The pre-configuration tasks consist of launching the installation wizard, providing licensing and activation details, pre-scanning the server for viruses, and choosing an installation type.

To start the pre-configuration tasks:

1. Open the folder that contains the setup files and double-click **Setup** (`SETUP.EXE`). The **Client Server Messaging Welcome** screen appears.

FIGURE 4-1. Client Server Security Welcome Screen

2. Click **Next**. The **Software License Agreement** screen appears.
3. Read the license agreement. If you agree with the terms, select **I accept the terms in the license agreement**.
4. Click **Next**. The **Product Activation** screen appears.

FIGURE 4-2. Product Activation Screen

Trend Micro Installation for SMB

Product Activation
Activate your product to enable scanning and security updates.

Step 1. Register Online
Use the Registration Key that came with your product and click the button below to register online. An Activation Code will be sent to you via email. (Skip this step if you already have the Activation Code).

Register Online

Step 2. Activate
Enter the Activation Code you receive from registration to activate your product.

Activation Code:

InstallShield

< Back Next > Cancel

5. Click **Register Online** if your product is not been registered yet. If the product is already registered, skip this step.
6. Enter the Activation Code in the **Activation Code** field.

Note: If you do not have an **Activation Code**, click **Next** to install the trial version. Upgrade to the full version before the 30-day trial period ends and all settings will remain.

7. Click **Next**. The **Computer Prescan** screen appears.

FIGURE 4-3. Computer Prescan Screen

8. Choose whether to prescan your computer for threats by selecting one of the following options:
 - Prescan my computer for threats
 - Do not prescan my computer for threats

Note: If you choose to prescan your computer for threats, a threat progress screen will appear while scanning is taking place. See [Actions for Prescan Detections](#) on page 4-7.

9. Click **Next**. The **Setup Type** screen appears.

FIGURE 4-4. Installation Setup Type Screen

10. From the **Setup Type** screen, choose one of the following options:

- Typical installation (recommended)
- Custom installation

Note: For instructions on performing an installation using the Typical method, see *Performing a Typical Installation* on page 4-28. The default values for the Custom installation are exactly the same as the values for a Typical installation.

11. Click **Next**. The **Setup Overview** screen appears. At this time, all of the pre-installation tasks are complete.

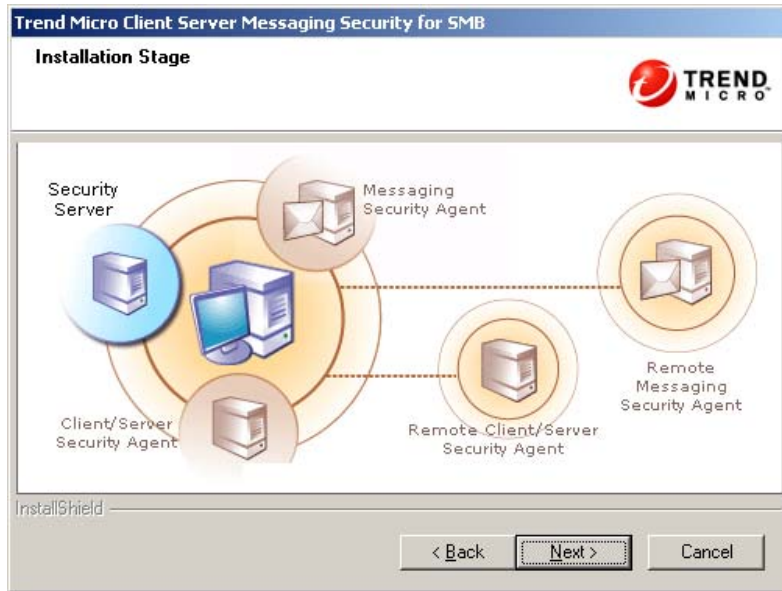
FIGURE 4-5. Installation Setup Overview Screen

12. The **Setup Overview** screen briefly lists the tasks that you need to complete in order to install the Trend Micro Security Server, Security Dashboard, and Client/Server Security Agent.

Part 2 – Configuring the Security Server and Security Dashboard Settings

To configure the Security Server and Security Dashboard:

1. From the **Setup Overview** screen, click **Next**. The **Installation Stage** screen appears with the Security Server icon highlighted.

FIGURE 4-6. Security Server Installation Stage Screen

2. Click **Next**. The **Server Identification** screen appears.

FIGURE 4-7. Security Server Identification Screen

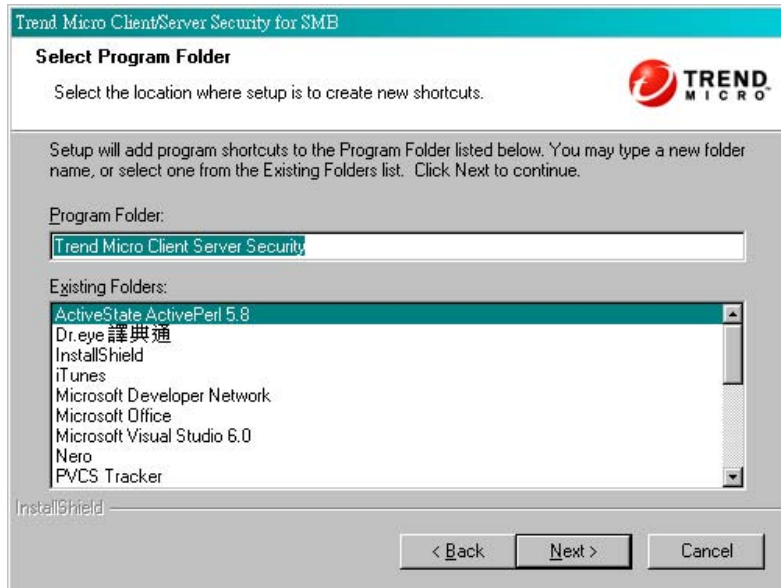
3. Choose from one of the following server identification options for client-server communication:
 - **Server information** – Choose Domain name or IP address:
 - **Domain name** – Verify the target server domain name. You can also use the server's fully qualified domain name (FQDN) if necessary to ensure successful client-server communication.
 - **IP address** – Verify that the target server IP address is correct.

Tip: Clicking **IP address** is not recommended if the computer the Security Server will be installed on obtains an IP address from a DHCP server. If the server has multiple network interface cards (NICs), Trend Micro recommends using one of the IP addresses, instead of the domain name or FQDN.

- **Target directory** – Enter the target directory where Trend Micro Security Server files will be installed.

4. Click **Next**. The **Select Program Folder** screen appears.

FIGURE 4-8. Select Program Folder Screen



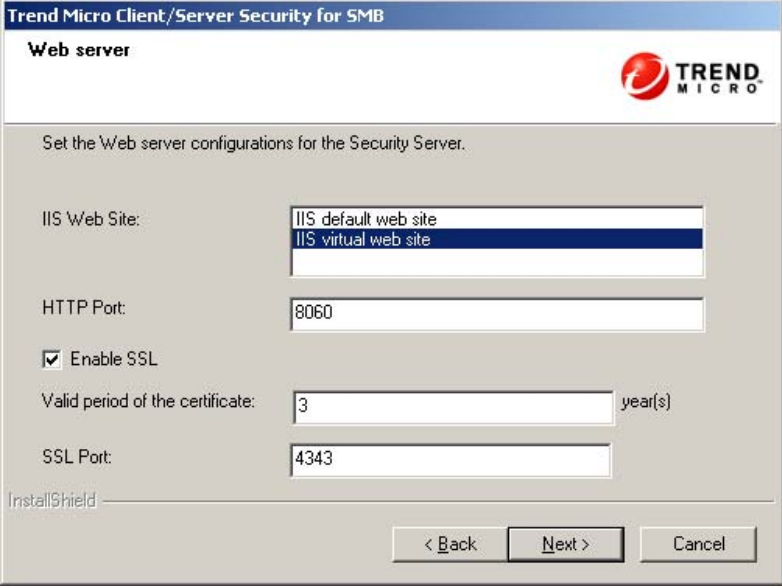
Note: This screen will not appear if you choose the Typical installation method.

5. Type a location in the **Program folder** field where program shortcuts will be stored or accept the default location.
6. Click **Next**. The **Web Server** screen appears allowing you to choose a Web server

FIGURE 4-9. Web Server Selection Screen

Note: This screen will not appear if you choose the Typical installation method.

7. From the **Web Server** screen, select a Web server to host the Security Dashboard. Choose from one of the following:
 - IIS server
 - Apache web server
8. Click **Next**. Depending on the type of server chosen, the corresponding screen appears.

FIGURE 4-10. IIS Web Server Configuration Screen

The screenshot shows a configuration window titled "Trend Micro Client/Server Security for SMB". The window has a "Web server" tab selected. The main heading is "Web server" with the Trend Micro logo to its right. Below this, a subtitle reads "Set the Web server configurations for the Security Server." The configuration fields are as follows:

- IIS Web Site:** A dropdown menu with "IIS default web site" and "IIS virtual web site" (the latter is highlighted).
- HTTP Port:** A text box containing "8060".
- Enable SSL:** A checkbox that is checked.
- Valid period of the certificate:** A text box containing "3" followed by the label "year(s)".
- SSL Port:** A text box containing "4343".

At the bottom left, the text "InstallShield" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

FIGURE 4-11. Apache Web Server Configuration Screen

Note: This screen will not appear if you choose the Typical installation method.

9. Configure the following Web server settings:

- HTTP port
- Enable SSL
- SSL port

Note: If using IIS server, you must specify an IIS Web site, **virtual** or **default**. Client Server Messaging will assign default values for the HTTP and SSL port settings.

10. Click **Next**. The **Proxy Server** screen appears.

FIGURE 4-12. Proxy Server Settings Screen

Trend Micro Client/Server Security for SMB

Proxy Server

If you use a proxy server to connect to the Internet, enter your proxy information in the fields provided. Security Server uses this information to connect to the Trend Micro update server to download updates.

☐ Use a proxy server

Proxy type: HTTP Proxy

Server name or IP address:

Port:

User name:

Password:

InstallShield

< Back Next > Cancel

Note: This screen will not appear if you choose the Typical installation method.

11. If a proxy server is required to access the Internet, select the **Use a proxy server** check box, and then provide the following information:
 - Proxy type
 - Server or IP address
 - Port
 - User name
 - Password
12. Click **Next**. The **SMTP Server and Notification Recipient(s)** screen appears.

FIGURE 4-13. SMTP Server Settings Screen

The screenshot shows a window titled "Trend Micro Client Server Messaging Security for SMB" with a sub-header "SMTP Server and Notification Recipient(s)". The Trend Micro logo is in the top right. Below the header, it says "Setup the SMTP server for sending all notifications and reports generated by Trend Micro Security Server." There are three input fields: "SMTP server:" with the value "192.168.1.2", "Port:" with the value "25", and "Recipient(s):" with the value "user@NotRealSite.com". Below the recipient field, a note says "(Use semicolon';' to separate multiple addresses. For example: user1@domain.com;user2@domain.com)". At the bottom left is the "InstallShield" logo, and at the bottom right are three buttons: "< Back", "Next >", and "Cancel".

13. The **SMTP Server and Notification Recipient(s)** screen, requires the following information:

- SMTP Server
- Port
- Recipient(s)

Note: The installation program will automatically detect the name of the SMTP server and fill in the **SMTP Server** and **Port** fields if the SMTP server is on the same computer as the Security Server installation.

14. Click **Next**. The **Administrator Account Password** screen appears.

FIGURE 4-14. Administrator Account Password Screen

Trend Micro Client Server Messaging Security for SMB

Administrator Account Password

Type a password and confirm that password in the field provided.

Protect the Security Server Web console and clients with passwords to prevent unauthorized users from modifying your settings or removing your clients.

Security Server Web console:

Password:

Confirm Password:

Client/Server Security Agents:

Password:

Confirm Password:

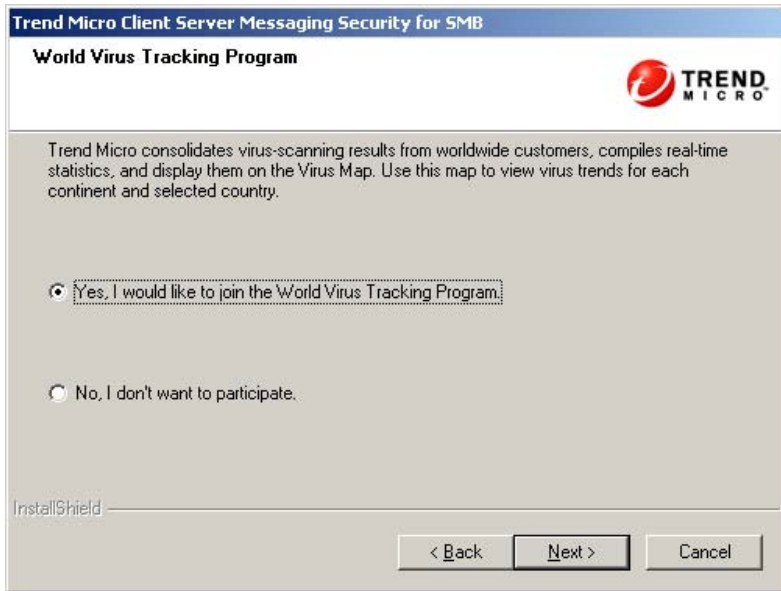
InstallShield

< Back Next > Cancel

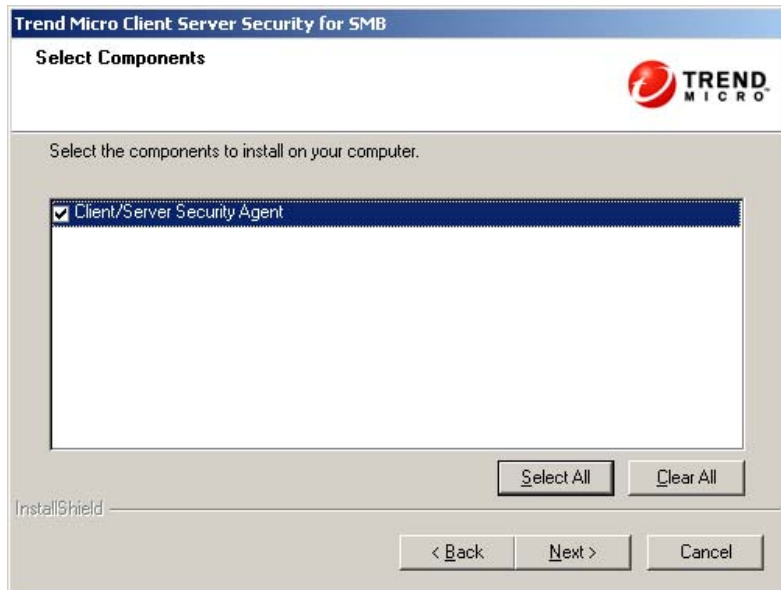
15. The **Administrator Account Password** screen requires the following information:
- **Security Dashboard** – Needed in order to administer the Security Dashboard
 - Password
 - Confirm password
 - **Client/Server Security Agent** – Needed in order to uninstall the Client/Server Security Agent
 - Password
 - Confirm password

Note: The Password field holds 1 – 24 characters, and is case sensitive.

16. Click **Next**. The **World Virus Tracking Program** screen appears.

FIGURE 4-15. World Virus Tracking Program Screen

17. Choose whether to participate in the World Virus Tracking Program.
18. Click **Next**. The **Component Selection** screen appears.

FIGURE 4-16. Component Selection Screen

19. Select **Client/Server Security Agent**.
20. Click **Next**.

Part 3 – Configuring the Client Security Agents

The options below are dependent upon the components selected from the Component Selection screen. For example, if the local server already has the CSA installed, the option to install and configure the CSA will not appear.

To configure the CSAs:

1. Click **Next**. The **Client/Server Security Agent Installation Stage** screen appears with the CSA and Remote CSA icons highlighted.

FIGURE 4-17. Client/Server Security Agent Installation Stage Screen

Note: This screen will not appear if you choose the Typical installation method.

2. Click **Next**. The **Client/Server Security Agent Installation Path** screen appears.

FIGURE 4-18. Client/Server Security Agent Installation Path Screen

Trend Micro Client/Server Security for SMB

Client/Server Security Agent Installation Path

Type the directory path to specify where to install all clients. Note: You cannot change the directory path once master setup is complete. Ensure that the directory path you type is correct.

Use one of the following variables to set the client installation path:

- \$BOOTDISK: The drive letter of the boot disk
- \$WINDIR: The directory where Windows is installed
- \$ProgramFiles: The programs folder

If you do not want to use these default variables, you may specify a different installation path below.

Install all Client/Server Security Agents to the following path:

Check that this port does not conflict with your network environment. If this port number conflicts with your network environment, type a compatible number in the field.

Port number:

InstallShield

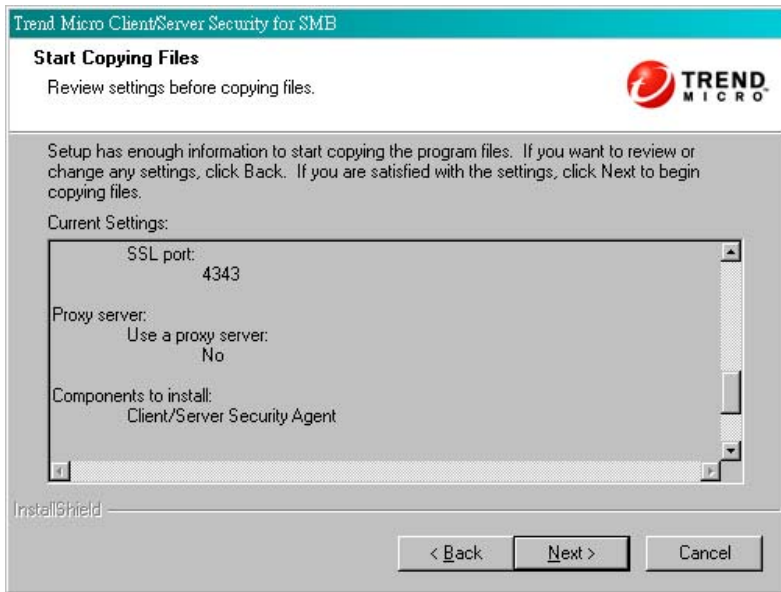
< Back Next > Cancel

Note: This screen will not appear if you choose the Typical installation method.

3. Set the following items:
 - Path – Directory where the CSA files are installed
 - Port – The port used for CSA and Security Server communications

Note: The Client/Server Security Agent applies the Path and Port settings to both local and remote clients.

4. Click **Next**. The **Review Settings** screen appears.

FIGURE 4-19. Review Settings Screen

5. Click **Next**. The installation process begins installing the Security Server and CSA.

Performing a Typical Installation

The Typical installation method follows the same flow as the Custom installation method. During a Typical installation the following options are not available because they use the Trend Micro default settings:

- Client Server Security program folder
- Web server
- Web server settings
- Proxy server settings
- Client/Server Security Agent settings

To perform an installation using the Typical method follow the steps in *Performing a Custom Installation* on page 4-9.

Performing a Silent Installation

Use the Silent installation method when multiple repeated installations using the same configuration are required.

You can use Silent installation to help you run multiple identical installations on separate networks. The procedure for running a silent installation is identical to the Custom installation except for the following pre-configuration and actual installation steps.

Pre-configuration steps:

1. Open the command window. Go to the directory where the Client Server Messaging Security setup files are located.
2. At the prompt, type **setup -r**.

To continue with the setup process and to learn more about configuring Client Server Security during installation see *Performing a Custom Installation* on page 4-9.

Starting the silent installation:

1. Go to:
 - For Win2000 OS – C:\WINNT
 - For WinXP/2003 OS – C:\Windows
2. Find the file **setup.iss** and copy it to the Client Server Messaging Security setup folder.
3. Open a command window and at the prompt navigate to the Client Server Messaging Security setup folder and type **setup -s**.

To verify that the installation is successful, go to the Client Server Messaging Security folder and view the **setup.log** file. If the result code is equal to "0", the installation was successful.

Upgrading Client Server Security

You can upgrade to a full version of Client Server Security from a previous version or from a trial version (see [Full Version and Trial Version](#) on page 4-4 for more information on the differences between the full and trial versions).

Upgrading from a Previous Version

Client Server Security supports the following upgrades:

- Upgrade from Client/Server Security 3.0 (SP1) to Client Server Security 3.6
- Upgrade from Client/Server Security 3.0 (SP1) to Client Server Messaging Security 3.6
- Upgrade from Client Server Security 3.5 to Client Server Security 3.6
- Upgrade from Client Server Security 3.5 to Client Server Messaging Security 3.6
- Upgrade from Client/Server/Messaging Security 3.0 (SP1) to Client Server Messaging Security 3.6
- Upgrade from Client Server Messaging Security 3.5 to Client Server Messaging Security 3.6

Note: If you upgrade the Client/Server Suite Server or Client Server Security Server that is running on a Windows NT4 server, the upgrade process will be interrupted and a warning message will appear. This happens as well if you upgrade Client/Server Agent on a Windows 9x/NT client. If you continue with the upgrade, the Client/Server Agent will be unable to report to the CS Server.

Client Server Security 3.6 does not support upgrade under the following conditions:

- Upgrade to Client Server Security 3.6 from OfficeScan Enterprise Edition or ScanMail for Microsoft Exchange.
- Upgrade from one language to another.
- Client Server Security 3.6 will not upgrade Client/Server Security Agents running on Windows 9x/ME/NT clients.
- Upgrade from Client/Server Suite 2.0 to Client Server Security 3.6
- Upgrade from Client/Server Suite 2.0 to Client Server Messaging Security 3.6

- Upgrade from Client/Server/Messaging Suite 2.0 to Client Server Messaging Security 3.6

Tip: You can preserve your client settings when you upgrade to this version of Client Server Security or if you need to reinstall this version. Trend Micro recommends deleting all virus log files from the Trend Micro Security Server before upgrading. If you want to preserve the virus log files, save them to another location first.

To upgrade to this version of Client Server Security:

- Run the master installer program on the target computer. Upgrading is very similar to performing a fresh install, but you will not be prompted to enter configuration information, such as port numbers or proxy server information. Client Server Security uses the same existing configuration information on the computer (see *Performing a Custom Installation* on page 4-9 for instructions).

Upgrading from an Evaluation Version

When your trial version is about to expire, Client Server Security display a notification message on the **Live Status** screen. You can upgrade from a trial version to the full version using the Security Dashboard. Your configuration settings will be saved. When you purchase a license to the full version, you will be given a Registration Key or an Activation Code.

To upgrade from a trial version:

1. Open the Security Dashboard.
2. On the main menu, click **Preferences > Product License**. The **Product License** screen appears.
3. Click **View license upgrade instructions**.
4. If you have an Activation Code, click **Enter a new code**.
5. Type the activation code in the **New Activation Code** field and click **Activate**.
If you do not have an Activation Code, click **Register Online** and use the Registration Key to obtain an Activation Code.

Verifying the Trend Micro Security Server Installation or Upgrade

After completing the installation or upgrade, verify that the Trend Micro Security Server is properly installed.

To verify the installation, do the following:

- Look for the Client Server Security program shortcuts on the Windows **Start** menu of the Trend Micro Security Server
- Check if Client Server Security is in the **Add/Remove Programs** list of the Client Server Security Control Panel
- Log on to the Security Dashboard with the server's URL:

```
http://{Client Server Security_server_name}:{port  
number}/SMB
```

or if using SSL:

```
https://{Client Server Security_server_name}:{port  
number}/SMB
```

where {Client Server Security_server_name} is the name or IP address you designated.

Uninstalling the Trend Micro Security Server

Client Server Security uses an uninstall program to safely remove the Trend Micro Security Server from your computer. Remove the Client/Server Security Agent program from all clients before removing the server.

To remove the Trend Micro Security Server:

1. On the computer you used to install the server, click **Start > Control Panel > Add or Remove Programs**.
2. Click **Trend Micro Security Server for SMB**, 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.
5. Click **OK** to close the uninstallation program.

Note: Uninstalling the Trend Micro Security Server does not uninstall clients. Uninstall or move all clients before uninstalling the Trend Micro Security Server.

Installing the Trend Micro Client/Server Security Agent

This chapter explains the steps necessary for successful Trend Micro Client/Server Security Agent installation and upgrade. It also provides information on removing the Client/Server Security Agent program.

The topics discussed in this chapter include:

- *Choosing an Installation Method* on page 5-2
- *Installing from the Internal Web Page* on page 5-4
- *Installing with Login Script Setup* on page 5-5
- *Installing with Windows 2000/Server 2003 Scripts* on page 5-7
- *Installing with Client Packager* on page 5-8
- *Sending the Package via Email* on page 5-11
- *Installing with an MSI File* on page 5-12
- *Installing with Windows Remote Install* on page 5-12
- *Installing with Vulnerability Scanner* on page 5-14
- *Upgrading the Client/Server Security Agent* on page 5-16

- *Migrating from Third-party Antivirus Applications* on page 5-17
- *Verifying the Client Installation, Upgrade, or Migration* on page 5-22
- *Removing the Client Using its Uninstallation Program* on page 5-25

Choosing an Installation Method

Trend Micro Client Server Security for SMB provides several methods to install the Client/Server Security Agent. This section provides a summary of the different methods.

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

- **Internal Web page** – Instruct the users in your organization to go to the internal Web page and download the Client/Server Security Agent setup files (see *Installing from the Internal Web Page* on page 5-4)
- **Login Script Setup** – Automate the installation of the Client/Server Security Agent to unprotected computers when they log on to the domain (see *Installing with Login Script Setup* on page 5-5)
- **Client Packager** – Deploy the Client/Server Security Agent setup or update files to clients via email (see *Installing with Client Packager* on page 5-8)
- **Windows Remote Install** – Install the Client/Server Security Agent program on all Windows Vista/2000/XP/Server 2003 clients from your Web console (see *Installing with Windows Remote Install* on page 5-12)
- **Trend Micro™ Vulnerability Scanner (TMVS)** – Install the Client/Server Security Agent on all Windows Vista/2000/XP (Professional)/Server 2003 clients

with the Trend Micro Vulnerability Scanner (*Installing with Vulnerability Scanner* on page 5-14)

TABLE 5-1. Trend Micro Client/Server Security Agent Deployment Methods

	Web page	Login scripts	Client packager	Windows Remote Install	TMVS
Suitable for deployment across the WAN	Yes	No	Yes	No	No
Suitable for centralized administration and management	Yes	Yes	No	Yes	Yes
Requires client user intervention	Yes	No	Yes	No	No
Requires IT resource	No	Yes	Yes	Yes	Yes
Suitable for mass deployment	No	Yes	No	Yes	Yes
Bandwidth consumption	Low, if scheduled	High, if clients are started at the same time	Low, if scheduled	Low, if scheduled	Low, if scheduled

To use any of these Client/Server Security Agent deployment methods, you must have local administrator rights on the target computers.

Installing, Upgrading, or Migrating Client/Server Security Agent

This section provides information on the following:

- Performing a fresh Client/Server Security Agent install with your chosen installation method (see *Choosing an Installation Method* on page 5-2)
- Upgrading from a previous version of Client/Server Security Agent to the current version (see *Upgrading the Client/Server Security Agent* on page 5-16)
- Migrating from a third-party antivirus installation to the current version of Client/Server Security Agent (see *Migrating from Third-party Antivirus Applications* on page 5-17)

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

Performing a Fresh Install

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

Installing from the Internal Web Page

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

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

Tip: You can use Vulnerability Scanner to see which clients have not followed the instructions to install from the Security Dashboard (see [Using Vulnerability Scanner to Verify the Client Installation](#) on page 5-22 for more information).

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

To install from the internal Web page:

1. Open an Internet Explorer window and type one of the following:
 - Trend Micro Security Server with SSL:
`https://{Trend Micro Security Server_name}:{port}/SMB/console/html/client`
 - Trend Micro Security Server without SSL:
`http://{Trend Micro Security Server_name}:{port}/SMB/console/html/client`
2. Click **Install Now** to start installing the Client/Server Security Agent.

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

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

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

Installing with Login Script Setup

Use Login Script Setup to automate the installation of the Client/Server Security Agent on unprotected computers when they log on to the domain. Login Script Setup

adds a program called `autopcc.exe` to the server login script. The program `autopcc.exe` performs the following functions:

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

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

Note: Windows Vista does not support this feature.

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

1. On the computer you used to run the server installation, Open **C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\SetupUsr.exe**
2. The **Login Script Setup** utility loads. The console displays a tree showing all domains on your network.
3. Browse for the Windows 2000/Server 2003 computer whose login script you want to modify, select it, and then click **Select**. The server must be a primary domain controller and you must have administrator access.

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

4. Type your user name and password. Click **OK** to continue.

The **User Selection** screen appears. The **Users** list shows the computers that log on to the server. The **Selected users** list shows the users whose computer login script you want to modify.

- To modify the login script of a single user or multiple users, select them from **Users** and then click **Add**
- To modify the login script of all users, click **Add All**
- To exclude a user whose computer you previously modified, select the name in **Selected users** and click **Delete**

- To reset your choices, click **Delete All**
5. Click **Apply** when all the target users are in the **Selected users** list.
A message appears informing you that you have modified the server login scripts successfully.
 6. Click **OK**. The Login Script Setup utility will return to its initial screen.
 - To modify the login scripts of other servers, repeat steps 2 to 4
 - To close Login Script Setup, click **Exit**

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

Installing with Windows 2000/Server 2003 Scripts

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

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

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

where:

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

`ofcscan` is the shared name of the PCCSRV folder where the `autopcc.exe` is located.

The Windows 2000 login script is on the Windows 2000 server (through a net logon shared directory), under:

```
\\Windows 2000 server\system
drive\WINNT\SYSTEM32\domain\scripts\ofcscan.bat
```

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

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

Installing with Client Packager

Client Packager can compress setup and update files into a self-extracting file to simplify delivery via email, CD-ROM, or similar media. It also includes an email function that can open your Microsoft™ Outlook address book and allow you to send the package from within the Client Packager console.

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

Note: Client packager requires a minimum of 140MB free disk space on the client. Windows Installer 2.0 is necessary for the client to run an MSI package.

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

- **Executable** – This common file type has an `.exe` extension

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

- **Microsoft Installer Package Format (MSI)** – This file type conforms to the Microsoft Windows Installer package specifications. For more information on MSI, see the Microsoft Web site.

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

Note: Install **Microsoft Outlook** to use the Client Packager send mail option.

To create a package with the Client Packager GUI:

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

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

4. In **Target operating system**, select the operating system for which you want to create the package.
5. Select the type of package you want to create:
 - **Setup** – Select if installing the Client/Server Security Agent program.
 - **Update** – Select if updating Client/Server Security Agent components only.
6. Select from among the following installation options under **Options**:
 - **Silent Mode** – Creates a package that installs on the client machine in the background, unnoticeable to the client. The installation status window will not appear.
 - **MSI Package** – Creates a package that conforms to the Microsoft Windows Installer Package Format.

Note: If you select MSI Package, the package file has an `.msi` extension; otherwise, it has an `.exe` extension. The MSI package is for Active Directory deployment only. For local installation, create an `.exe` package.

- **Disable Prescan (only for fresh-install)** – Disables the normal file scanning that Client Server Security performs before starting setup.
7. Under **Components**, select the components to include in the installation package:
 - **Program** – All components (if you select **Program**, Client Packager automatically selects the other components).
 - **Virus pattern**– A file that helps Client Server Security identify virus signatures– unique patterns of bits and bytes that signal the presence of a virus.

- **Virus scan engine 32-bit** – The engine Client Server Security uses to scan for viruses.
 - **Virus scan engine 64-bit** – The engine Client Server Security uses to scan for viruses
 - **Virus cleanup template** – Used by the virus cleanup engine, this template helps identify viruses, Trojans and Trojan processes.
 - **Virus cleanup engine 32-bit** – The engine Damage Cleanup Services™ uses to scan for and remove from memory viruses, Trojans and Trojan processes, and other malware.
 - **IntelliTrap exception pattern**
 - **IntelliTrap pattern**
 - **Vulnerability pattern** – A file that helps Client Server Security identify vulnerabilities on client machines.
 - **Common firewall pattern** – Like the virus pattern file, this file helps Client Server Security identify virus signatures.
 - **Common firewall engine 32-bit** – The driver the Personal Firewall uses with the network virus pattern file to scan client machines for network viruses.
 - **Spyware Pattern** – Contains known spyware signatures and used by the spyware scan engines (both 32-bit and 64-bit) to detect spyware on clients and servers for manual and scheduled scans
 - **Spyware Active-monitoring Pattern** – Similar to spyware pattern, but is used by the scan engine for real-time anti-spyware scanning
 - **Spyware Scan Engine (32-bit)** – A separate scan engine that scans for, detects, and removes spyware from infected clients and servers running on i386 (32-bit) operating systems (for example, Windows Vista, Windows 2000, and Windows XP)
 - **Spyware Scan Engine (64-bit)** – Similar to the spyware scan engine for 32-bit systems, this scan engine scans for, detects, and removes spyware on x64 (64-bit) operating systems (for example, Windows Vista x64, Windows XP Professional x64 Edition, Windows 2003 x64 Edition)
 - **Anti-Rootkit Driver (32-bit)** – A module required by the spyware scan engine to detect rootkits
8. Select the Client/Server Security Agent utilities to include in the package:

- **POP3 Mail Scan** – Performs a virus scan on the client's Post Office Protocol 3 (POP3) mail messages and attachments as they are downloaded from the mail server.
9. Ensure that the location of the `ofcscan.ini` file is correct next to **Source file**. To modify the path, click  to browse for the `ofcscan.ini` file. By default, this file is located in the `\PCCSRV` folder of the Trend Micro Security Server.
 10. In **Output file**, click  to specify the file name (for example, `ClientSetup.exe`) and the location to create the client package.
 11. Click **Create** to build the client package. When Client Packager finishes creating the package, the message "Package created successfully" appears. To verify successful package creation, check the output directory you specified.
 12. Send the package to your users via email, or copy it to a CD or similar media and distribute among your users.

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

Sending the Package via Email

Note: Microsoft Outlook is necessary to use the Client Packager email function.

To send the package from the console:

1. Click **Send mail**. The **Choose Profile** window appears.
2. Choose a profile name from the list and click **OK**.
3. Enter the user name and password required to access Outlook on your computer.
4. The **Send mail** screen opens with the default subject and message. Click **To** and specify the recipients of the package. Client Packager opens your Microsoft Outlook address book. Click **Cc** or **Bcc** to furnish copies to other recipients in your organization.
5. Edit the default subject and message (optional) and click **Send**.

Installing with an MSI File

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

For more information on MSI, see the Microsoft Web site (www.microsoft.com). For instructions on creating an MSI file, see *Installing with Client Packager* on page 5-8).

Installing with Windows Remote Install

Remotely install the Client/Server Security Agent to Windows Vista/2000/XP (Professional Edition Only) and Server 2003 computers connected to the network, and install to multiple computers at the same time. To use Windows Remote Install, you need administrator rights for the target computers.

Note: You cannot use Windows Remote Install to install the Client/Server Security Agent on machines running Windows XP Home Edition.

To install with Windows Remote Install:

Note: Installing CSA on Windows Vista requires a few additional steps. Refer to *Enabling CSA Remote Install on Windows Vista Clients* on page 5-13 for additional details.

1. From the Security Dashboard main menu, click **Security Settings > Add**. The **Add Computer** screen appears.
2. Select **Desktop or server** from under **Computer Type** and then select **Remote install** from under **Method**.
3. Click **Next**. The **Remote Install** screen appears.
4. From the list of computers in the **Groups and Computers** box, select a client, and then click **Add >>**. A prompt for a user name and password to the target computer appears. You need administrator rights to the target computer.

5. Type your user name and password, and then click **Login**. The target computer appears in the **Selected Computers** list box.
6. Repeat these steps until the list displays all the Windows computers in the **Selected Computer** list box.
7. Click **Install** to install the Client/Server Security Agent to your target computers. A confirmation box appears.
8. Click **Yes** to confirm that you want to install the client to the target computers. A progress screen appears as the program copies the Client/Server Security Agent files to each target computer.

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

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

Enabling CSA Remote Install on Windows Vista Clients

Installing CSA on Windows Vista clients requires additional steps.

To enable Remote Install on Windows Vista clients:

1. Temporarily enable File and Printer Sharing.

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

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

2. Temporarily start the Remote Registry service.

- a. Open Microsoft Management Console.

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

- b. Right-click **Remote Registry** and select **Start**.

3. If required, return to the original settings after installing Client/Server Security Agent on the Windows Vista client.

Installing with Vulnerability Scanner

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

This section explains how to install the Client/Server Security Agent program with Vulnerability Scanner. For instructions on how to use Vulnerability Scanner to detect antivirus solutions, see the Administrative Tools section of the *Administrator's Guide* and the Trend Micro Security Server online help.

Note: You can use Vulnerability Scanner on machines running Windows 2000 or Server 2003; however, the machines cannot be running Terminal Server. You cannot install the Client/Server Security Agent with Vulnerability Scanner if an installation of the Trend Micro Security Server is present on the same machine.

To install the Client/Server Security Agent with Vulnerability Scanner:

1. In the drive where you installed the Trend Micro Security Server, open the following directories: **Client Server Security > PCCSRV > Admin > Utility > TMVS**.
2. Double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears.
3. Click **Settings**. The **Settings** screen appears.

FIGURE 5-1. TMVS Settings Screen

Settings

Product Query
Select the check boxes for the antivirus products that you want to check for on your network. To avoid getting false alarms, we recommend selecting all check boxes.

☒ Check for all Trend Micro products
☒ ServerProtect (NT /Linux)
☒ OfficeScan Corporate Edition/ Security Server
☒ PortalProtect
☒ ScanMail for Exchange
☒ InterScan family
☒ PC-cillin

☒ Check for other antivirus solutions
☒ McAfee VirusScan ePolicy Orchestrator
☒ Norton AntiVirus Corporate Edition

Port settings:

Description Retrieval Settings
Click the retrieval method that you want to use for getting computer descriptions.

☐ Normal retrieval ☒ Quick retrieval
☐ Retrieve computer descriptions when available

Alert Settings

☐ Email results to the system administrator
☐ Display alert on unprotected computers

Save As CSV File

☐ Automatically save the results to a CSV file.
Specify a default folder where CSV files will be saved.
Folder:

Ping Settings

☒ Enable vulnerability Scanner pings computers on your network to get their status. Specify your ping settings here.
 Packet size (10 to 512 bytes) Timeout (10 to 5000 ms)
☒ Detect OS type by ICMP OS fingerprinting operation. (ICMP Echo code=19)
 This function maybe unsuccessful under the firewall environment.

Security Server Setting for (Install and Log Report): Specify an server. (e.g. MyServer)

Port:
☒ Auto-install Client/Server Security Agent for unprotected computer

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

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

Upgrading the Client/Server Security Agent

You can upgrade to a full version of Client Server Security from a previous version or from a trial version. When you upgrade the Trend Micro Security Server, clients are automatically upgraded.

Migrating from Trend Micro Anti-Spyware

If you have Trend Micro Anti-Spyware (TMASY) on the network, take note of the following:

- If you install the CS server on the same server as the TMASY server, the CS server setup program will not remove or upgrade the TMASY server. You need to manually remove the TMASY server before installing the CS server on the same machine.
- Removing the TMASY client before installing the Client/Server Security Agent (CSA) is not required. The CSA setup program will automatically remove the TMASY client when detected on the same client computer, and then install CSA.
- The anti-spyware settings for CSA and TMASY are different. After installing the CSAs, you may need to configure the anti-spyware settings to make them the same as your previous TMASY client settings. Refer to Table 5-2 for a comparison of the CSA and TMASY anti-spyware settings.

TABLE 5-2. Comparison of CSA and TMASY Anti-Spyware Settings

	Client/Server Security Agent	Trend Micro Anti-Spyware Client
Real-time Scan	Enabled	Disabled (Active Application Monitoring)
Default action	Clean	
Manual Scan		
Scan type	Full scan	Quick scan
Default action	Clean	Scan and do nothing (auto clean is disabled by default)
Scan on start	N/A	Enabled
Check network	N/A	Enabled
Scheduled Scan	Disabled	Enabled
Scan schedule	Every Monday	Daily
Scan time	12:30	23:00
Scan type	Full scan	Quick scan
Default action	Clean	Scan and do nothing (auto clean is disabled by default)

Migrating from Third-party Antivirus Applications

Migrating from third-party antivirus software to Client Server Security is a two-step process: the installation of the Trend Micro Security Server, followed by the automatic migration of the clients.

Automatic Client Migration

Automatic client migration refers to replacing existing third-party client antivirus software with the Client/Server Security Agent program. The client setup program automatically removes the third-party software on your client computers and replaces it with the Client/Server Security Agent.

Refer to Table for a list of third-party client applications that Client Server Security can automatically remove.

Note: Client Server Security only removes the following client installations, not server installations.

TABLE 5-3. Removable Third-party Client Applications

Trend Micro
PC-cillin™ (Internet Security) 2000 Virus Buster 2001, 2000, 2000 for NT ver.1.00- PccillinCorp NT client PccillinCorp 95 client
Symantec™
Norton™ Internet Security™ 2005, 2004, 2004 JP
Norton Antivirus™ CE 10.1 Norton Antivirus™ CE 10.0 Norton Antivirus™ CE 9.0 Norton Antivirus™ CE 8.1 server Norton Antivirus™ CE 8.0 9x Norton Antivirus™ CE 8.0 NT Norton Antivirus™ CE 7.5 NT Norton Antivirus™ CE 7.5 9x Norton Antivirus™ CE 7.0 NT Norton Antivirus™ CE 7.0 for Windows NT Norton Antivirus™ CE 6.524
Symantec Antivirus CE 9.0
Symantec Client Security 3.0 NT
Symantec Client Firewall 2004 9x/NT
Symantec LiveUpdate 2.6
LANDesk VirusProtect 5.0
McAfee™
VirusScan™ Enterprise 8.0, 7.1, 7.0, Virus Scan (MSPlus98), WebScanX v3.1.6, VirusScan ASaP, 95 {3.20,4.01,4.02, 4.03(#4023),4.03a (#4059)}, NT 4.03a (#4019), 5.15, 5.16, 5.21, 6.01, 4.5, 4.51, Thin Client (TC)
VirusScan Professional 9.0
Managed VirusScan
SpamKiller
SecurityCenter
Desktop Firewall 8.0
NetShield™ NT 4.03a (build #4014, #4019), 4.5 (Build #4062)

TABLE 5-3. Removable Third-party Client Applications

Internet Security Suite™ 6.0
ePOAgent™ 1000, 2000, 3000
Dr.Solomon™ 4.0.3 Dr.Solomon™ 4.0.3 NT Dr.Solomon™ 7.77, 7.95 NT
LANDesk™
VirusProtect™ 5.0
Computer Associates™
eTrustITM Agent 8.0
iTechnology iGateway 4.0
eTrustITM Server 8.0
eTrust AntiVirus™ 7.1
InocuLAN™ NT 4.5, 9.x, 4.53
eTrust InoculateIT™ 7.0, 6.0
InoculateIT™ Clients for Windows 6.0
InocuLAN™ 5
Cheyenne AntiVirus™ 9x, NT
Ahnlab™
V3 Pro™ 2000 Deluxe, 98, 98 Deluxe
Panda Software™
Platinum™ 7.0
Antivirus 2007 (and 2007+ Firewall Italian version)
Antivirus 6.0, Local Networks, Windows NT WS
Titanium Antivirus 2004
FileSecure
CVPSecure
FileSecure Workstation

TABLE 5-3. Removable Third-party Client Applications

F-Secure™
Anti-Virus™ 4.04, 4.08, 4.2, 4.3, 5.3
Backweb™
Management Agent™
Internet Shield
E-mail Scanning
Kaspersky™
Antivirus Personal 4.0, Workstation 3.5. 5.4
Sophos™
Anti-Virus NT, NT 5.0.3.
AutoUpdate 1.4.0
Anti-Virus 9x
Authentium™
Command AntiVirus™ win 2000/XP, 4.64 for win 9x/ME, 4.8, 4.9, 4.90.0 Standalone, 4.8, 4.9, 4.91.0 Enterprise,
Grisoft™
Grisoft AVG 6.0, 7.0
Others
PER Antivirus
The Hacker Anti-Virus 5.5
eSafe Desktop v3
Norman Virus Control
NOD32 AV
F-Prot for Windows
Tegam ViGUARD 9.25e for Windows NT
ViRobot 2k Professional

TABLE 5-3. Removable Third-party Client Applications

Command AV 4.93.8 Standalone
Command AV 4.93.8 Enterprise

Verifying the Client Installation, Upgrade, or Migration

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

To verify the installation, do the following:

- Look for the Client Server Security program shortcuts on the Windows **Start** menu of the client running the Client/Server Security Agent.
- Check if Client Server Security is in the **Add/Remove Programs** list of the client's Control Panel.
- Use Vulnerability Scanner (see *Using Vulnerability Scanner to Verify the Client Installation* on page 5-22).

Using Vulnerability Scanner to Verify the Client Installation

You can also automate Vulnerability Scanner by creating scheduled tasks. For information on how to automate Vulnerability Scanner, see the Client Server Security online help.

Note: You can use Vulnerability Scanner on machines running Windows 2000 and Server 2003; however, the machines cannot be running Terminal Server.

To verify client installation using Vulnerability Scanner:

1. In the drive where you installed the Trend Micro Security Server, open the following directories: **Trend Micro Security Server > PCCSRV > Admin > Utility > TMVS**. Double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears.
2. Click **Settings**. The **Settings** screen appears.

3. Under **Product Query**, select the **OfficeScan Corporate Edition/Security Server** check box and specify the port that the server uses to communicate with clients.
4. Under **Description Retrieval Settings**, click the retrieval method to use. Normal retrieval is more accurate, but it takes longer to complete.

If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting the **Retrieve computer descriptions when available** check box.

5. To have results automatically sent to yourself or to other administrators in your organization, select the **Email results to the system administrator** check box under **Alert Settings**. Then click **Configure** to specify your email settings.
 - In **To**, type the email address of the recipient.
 - In **From**, type your email address. If you are sending it to other administrators in your organization, this will let the recipients know who sent the message.
 - In **SMTP server**, type the address of your SMTP server. For example, type `smtp.company.com`. The SMTP server information is required.
 - In **Subject**, type a new subject for the message or accept the default subject.
6. Click **OK** to save your settings.
7. To display an alert on unprotected computers, select the **Display alert on unprotected computers** check box. Then click **Customize** to set the alert message. The **Alert Message** screen appears.
8. Type a new alert message in the text box or accept the default message and then click **OK**.
9. To save the results as a comma-separated value (CSV) data file, select the **Automatically save the results to a CSV file** check box. By default, Vulnerability Scanner saves CSV data files to the TMVS folder. If you want to change the default CSV folder, click **Browse**, select a target folder on your computer or on the network, and then click **OK**.
10. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout fields**.
11. Click **OK**. The Trend Micro Vulnerability Scanner console appears.

12. To run a manual vulnerability scan on a range of IP addresses, do the following:
 - a. In **IP Range to Check**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers.
 - b. Click **Start** to begin checking the computers on your network.
13. To run a manual vulnerability scan on computers requesting IP addresses from a DHCP server, do the following:
 - a. Click the **DHCP Scan** tab in the **Results** box. The **DHCP Start** button appears.
 - b. Click **DHCP Start**. Vulnerability scanner begins listening for DHCP requests and performing vulnerability checks on computers as they log on to the network.

Vulnerability Scanner checks your network and displays the results in the **Results** table. Verify that all desktop and notebook computers have the client installed.

If Vulnerability Scanner finds any unprotected desktop and notebook computers, install the client on them using your preferred client installation method.

Testing the Client Installation with the EICAR Test Script

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

<http://www.eicar.org>

The EICAR test script is an inert text file with a `.com` extension. It is not a virus and does not contain any fragments of viral code, but most antivirus software will react to it as if it were a virus. Use it to simulate a virus incident and confirm that email notifications, HTTP scanning, and virus logs work properly.

WARNING! *Never use real viruses to test your antivirus installation.*

To test the client installation with the EICAR test script:

1. Make sure Real-time scan is enabled on the client.
2. Copy the following string and paste it into Notepad or any plain text editor:
`X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. Save the file as EICAR.com to a temporary directory. Client/Server Security Agent should immediately detect the file.
4. To test other computers on your network, attach the EICAR.com file to an email message and send it to one of the computers.

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

To test the client installation HTTP scanning capability:

- Download the EICAR.com test script from either of the following URLs:
<http://www.trendmicro.com/vinfo/testfiles/>
http://www.eicar.org/anti_virus_test_file.htm

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

Removing the Client Using its Uninstallation Program

If you granted users the privilege to remove the client program, instruct them to run the client uninstallation program from their computers. For more information, see the Trend Micro Security Server online help.

To run the client uninstallation program:

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

3. Type the uninstall password and then click **OK**. The **Client Server Security Client Uninstallation** screen shows the progress of the uninstallation.

When uninstallation is complete, the message "Uninstallation is complete" appears.

The Trend Micro Security Dashboard for SMB

This chapter describes the main features, elements, and navigation methods of the Security Dashboard.

The topics discussed in this chapter include:

- *Exploring the Security Dashboard* on page 6-2
- *Getting Around the Security Dashboard* on page 6-3

Exploring the Security Dashboard

When you install the Trend Micro Security Server, you also install the Security Dashboard, which uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

To open the Security Dashboard:

1. On any computer on the network, open a Web browser and type the following in the address bar:

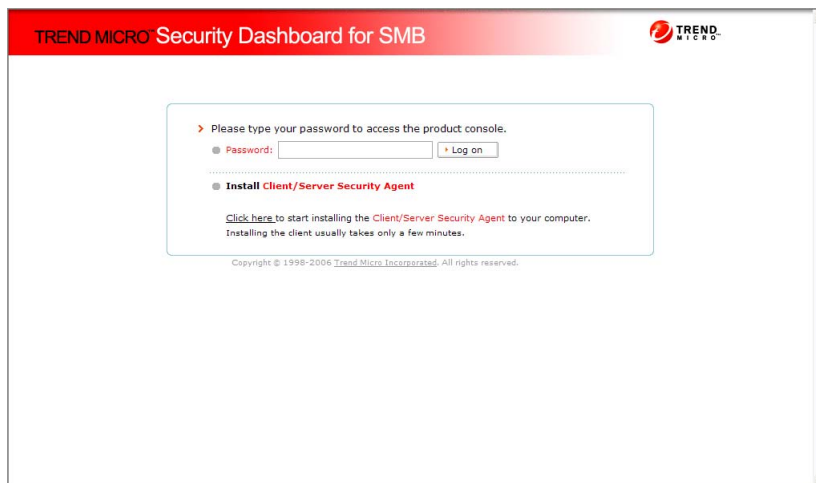
`http://{Client Server Security_Server_Name}:{port number}/SMB` in the address bar.

If using SSL, type the following in the address bar:

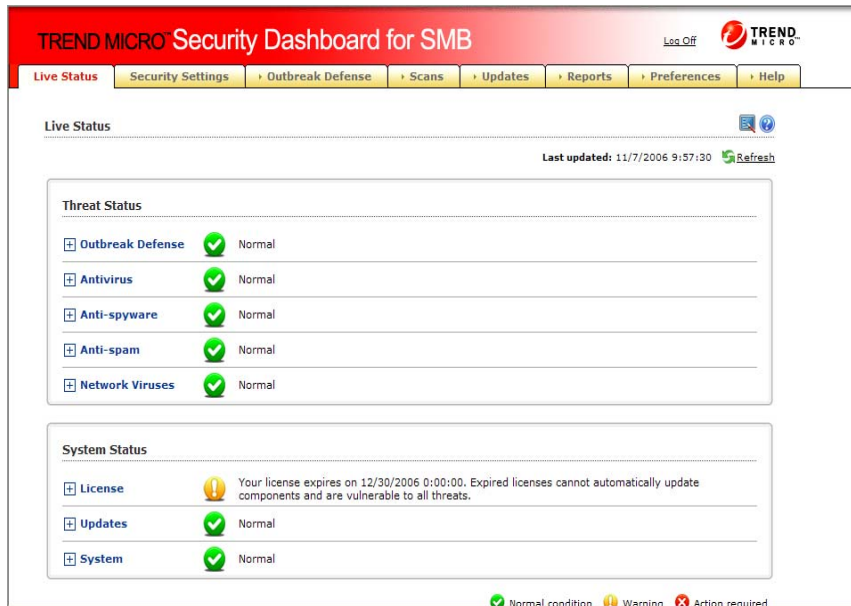
`https://{Client Server Security_Server_Name}:{port number}/SMB`

2. The browser displays the Trend Micro Security Dashboard for SMB login screen.

FIGURE 6-1. Login Screen of the Security Dashboard



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

FIGURE 6-2. Live Status Screen

Getting Around the Security Dashboard

There are two main parts to the Security Dashboard: the main navigation menu and the main body frame. Some screens contain a side menu and a tool bar.

The main navigation menu contains the following sections:

Live Status

- View the latest threats to client computers and servers.
- Deploy updates to at-risk clients.
- Monitor server disk space.

Security Settings

- Configure security setting for client computers and servers.
- Replicate settings from one computer or server to another.

- Install protection to client computers and servers.
- Configure the Spyware/Grayware Approved List (can also be configured from **Scans**)

Outbreak Defense

- View recent virus outbreak activity.
- Scan client computers and servers for vulnerabilities.
- View the vulnerability level of different client computers and servers.
- Detect vulnerabilities on clients, servers, and mail servers.
- View and clean-up client computers and servers that are infected with viruses or other malware.

Scans

- Scan client computers and servers for viruses, spyware, and other malicious applications.
- Configure the Spyware/Grayware Approved List (can also be configured from **Security Settings**)
- Schedule scans of client computers and servers.

Updates

- Check the Trend Micro ActiveUpdate server for the latest updated components, including virus pattern files, virus scan engine, spyware pattern, spyware scan engine, anti-rootkit driver, spyware active-monitoring pattern, program files, and Damage Cleanup scan engine and template.
- Configure update source.
- Configure update schedule.
- Assign and configure update agents.

Preferences

- Set up notifications for different events that occur.
- Configure global settings for ease of maintenance.
- Use different client and administrative tools to help manage security for the network and clients.

- View product license information, maintain the administrator password, and help keep the global business environment safe by joining the World Virus Tracking program.

Help

- Use the help menu to get answers to Client Server Security questions, view other Trend Micro security solutions, and get customer support.

Configuring Desktop and Server Groups

This chapter explains how to set Real-time scan options, configure Personal Firewall settings, set desktop privileges, and specify a quarantine directory for desktop and server groups.

The topics discussed in this chapter include:

- *Configurable Options for Desktop and Server Groups* on page 7-2
- *Configuring Real-time Scan* on page 7-2
- *Using the Personal Firewall* on page 7-8
- *Using Desktop Privileges* on page 7-16
- *Using Quarantine* on page 7-19

Configurable Options for Desktop and Server Groups

The following items can be accessed by clicking the Configure tool:

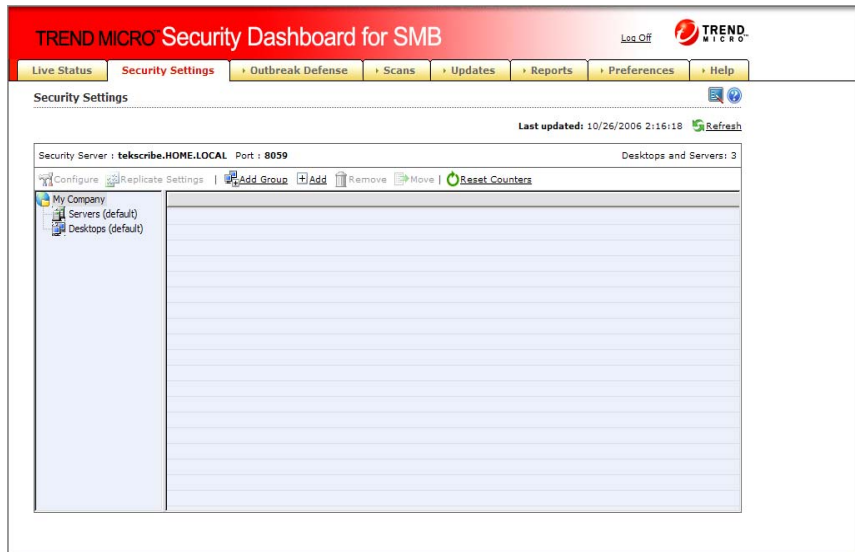
- **Antivirus/Anti-spyware** – Configure real-time scan antivirus and anti-spyware options for all members of the group.
- **Firewall** – Configure Personal Firewall options for all members of the group.
- **Client Privileges** – Configure privileges for all members of the group.
- **Quarantine** – Specify Quarantine directory for all members of the group.

Configuring Real-time Scan

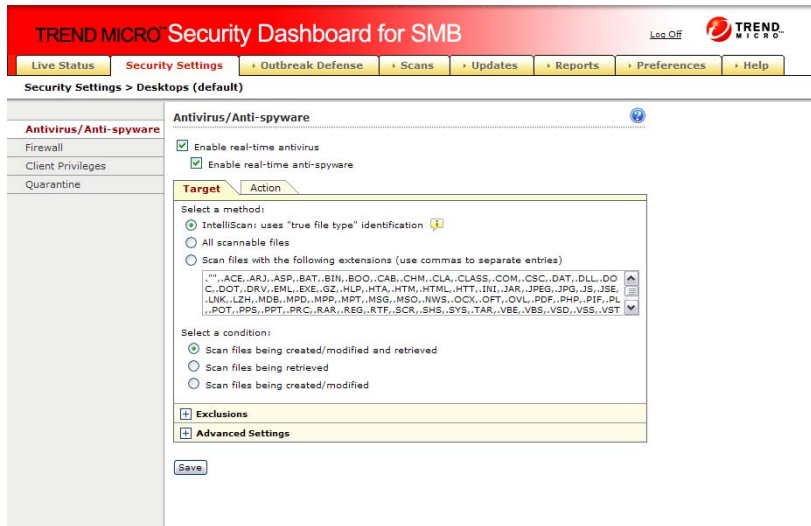
Use the **Configure** tool on the Security Settings page to set real-time scan settings for all members of the group.

To configure Real-time scan:

1. On the main menu, click **Security Settings**. The **Security Settings** screen appears.

FIGURE 7-1. Security Settings Screen

2. From the **Security Settings** screen, select a group, and then click the **Configure** tool. The **Configure** screen for the selected group appears with the **Antivirus/Anti-spyware** configuration options displayed by default.

FIGURE 7-2. Security Settings - Desktop/Server Configuration Screen

3. To enable antivirus real-time scan, select the **Enable real-time antivirus** check box.
4. To enable anti-spyware real-time scan, select the **Enable real-time anti-spyware** check box.
5. Select the **Target** tab to specify settings for the following options:
 - **All scannable files** – Click to scan all files that the client opens or saves
 - **Use IntelliScan** – Uses **true file type** identification – Click to use IntelliScan (see *Trend Micro IntelliScan* on page B-3).
 - **Scan files with the following extensions** – Click to manually specify the files to scan based on their extensions
You can add or delete extensions from the default set of extensions.

Tip: You can also use ? and * as wildcards when specifying extensions. For example, if you want to scan all files with extensions starting with D, you can type .D? or .D*. Client Server Security will scan all files with extensions starting with D, including .DOC, .DOT, and .DAT. This option is only available for Real-time Scan.

6. From the **Select a condition** section, choose one of the following conditions for scanning to occur:
 - **Scan files being created/modified and retrieved**
 - **Scan files being retrieved**
 - **Scan files being created/modified**
7. **Exclusions** – Select **Enable Exclusions** to exclude certain directories, files, and extensions from scanning. See [Excluding Files and Folders from Scans](#) on page 7-7.
8. **Advanced Settings** – Select **Advanced Settings** to choose the following advanced options:

For Antivirus Only

- **Enable IntelliTrap** – (Default)
- **Scan mapped drives and shared folders on the network**
- **Scan floppy during system shutdown**
- **Scan compressed files: Up to {number} compression layers**

For Anti-spyware Only

- Click the **Modify Spyware/Grayware Approved List** link to add to or modify the list of spyware/grayware applications that are allowed to run on clients and servers that belong to the group.
 - i. Use **Search** or the **Quick Find** links to locate the spyware/grayware application that you want to allow.
 - ii. Select the application name in the left pane. To select multiple applications, press CTRL while clicking the application names.
 - iii. Click **Add**.
9. Click **Save** to go back to the antivirus/anti-spyware security settings page.

10. Click the **Action** tab, and then specify how to handle Internet threats when Client Server Security detects them. Scan actions for viruses and spyware are configured separately.

For Virus Detections

- **ActiveAction** – (see *Trend Micro ActiveAction* on page B-4).
- **Perform the same action for all detected Internet threats**
- **Customized action for the following detected threats**

In the **Action** list, select the action to perform on infected files. You can click **Pass**, **Delete**, **Rename**, **Quarantine**, and **Clean**. The recommended scan action is **Clean**.

In the **Action for Uncleanable Threats** list, select the action to perform if a threat is uncleanable.

Client Server Security only performs the uncleanable threats action if the primary action is not successful. You can select actions for the following types of Internet Threats (the default action is specified below):

- **Joke:** Quarantine
- **Worm/Trojan:** Quarantine
- **Virus:** Clean
- **Test virus:** Pass
- **Packer:** Quarantine
- **Other threats:** Clean
- **Backup detected file before cleaning** check box – Select this check box (recommended) to save a copy of the file before it is cleaned. This saves a copy of the infected file in the following directory on the client computer:

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

For Spyware Detection

- **Clean** – Remove any spyware detected by real-time scan
- **Deny Access** – Prevent spyware from being installed, accessed, or executed

WARNING! *Denying access does not remove the spyware threat from infected clients and servers.*

11. Click **Advanced Settings** to view advanced setting options.
 - To display an alert message on the client when a virus is detected, select **Display an alert message on the desktop or server when a virus is detected**.
12. Click **Save**.

Excluding Files and Folders from Scans

To increase the performance of scanning and to skip files that are causing false alarms, you can exclude certain files, folders, and file types from scanning. The items you add to the exclusion list will be skipped by Manual Scan, Real-time Scan, and Scheduled Scan.

To exclude files and folders from scanning:

1. On the main menu, click **Security Settings**, select a group, and click **Configure**. The Security Settings screen will appear.
2. To configure exclusion options, click the **Antivirus/Anti-spyware** link from the side menu. The main frame changes to display the Antivirus configuration options. By default, the **Target** tab is selected.
3. Click the expand button next to the **Exclusions** section. The section expands to display Exclusion configuration options.
4. Under **Exclusions**, make sure that the check box next to **Enable Exclusions** is selected.
5. To exclude all folders containing Trend Micro products and components, select the **Do not scan the directories where Trend Micro products are installed** check box. To view details about the Trend Micro products excluded see [Trend Micro Product Exclusion List](#) on page D-1.
6. To exclude specific directories, type the directory names under **Enter the directory path (E.g. c:\temp\ExcludeDir)** and click **Add**.

7. To exclude specific files by file name, type the file names, or the file name with full path under **Enter the file name or the file name with full directory path** (E.g. **ExcludeDoc.hlp**; **c:\temp\excldir\ExcludeDoc.hlp**) and click **Add**.

Note: All subdirectories in the directory path you specify will also be excluded.

8. Specify the files to exclude based on their extensions.

To use specified extensions, select the extensions to protect from the **Select file extension from the list**, and click **Add**.

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

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

9. To apply this setting to all future clients that will belong to the group you selected, click **Save**.

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

Using the Personal Firewall

Trend Micro Client Server Security for SMB has simplified the process of configuring the Personal Firewall. In this version of Client Server Security, there are two options to choose from when configuring the Personal Firewall, simple mode and advanced mode. Simple mode enables the firewall with the Trend Micro recommended default settings. Use advanced mode to customize the Personal Firewall settings.

Personal Firewall Features

Personal Firewall helps protect Client Server Security Windows Vista/2000/XP/Server 2003 clients from hacker attacks and network viruses by creating a barrier between the client and the network.

Personal Firewall Defaults for Simple Mode

Personal 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 your clients, such as the need to access the ScanMail for Microsoft Exchange Web console.

TABLE 7-1. Personal Firewall Default Settings

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

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

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

Traffic Filtering

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

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

Intrusion Detection System

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

- Too Big Fragment
- Ping of Death
- Conflicted ARP
- SYN flood
- Overlapping Fragment
- Teardrop
- Tiny Fragment Attack
- Fragmented IGMP
- LAND attack

Exceptions

Exceptions are comprised of specific settings that allow or block different kinds of traffic based on client port number(s) and IP address(es). You can configure a list of exceptions. The exceptions in the list override the **Security level** settings.

Exception settings include the following:

- **Action** – Block or allow all traffic that meets the exception criteria
- **Direction** – Inbound or outbound network traffic to/from the client.
- **Protocol** – The type of traffic: TCP, UDP, ICMP.
- **Port(s)** – Ports on the client computer on which to perform the action.
- **Computers** – The computers on the network to which the above traffic criteria apply.

Configuring Exceptions: An 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.

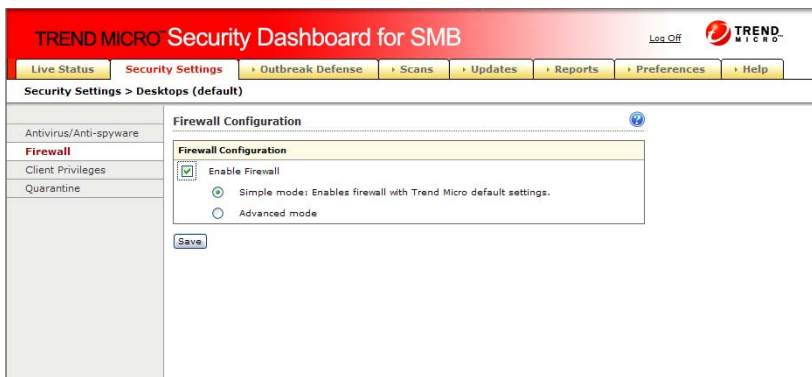
Configuring Personal Firewall – Simple Mode

This section provides the necessary steps for successful deployment of Personal Firewall. By default, Client Server Security disables the Personal Firewall on all new groups and clients.

To configure Personal Firewall:

1. On the main menu, select **Security Settings**. The **Security Settings** screen appears.
2. Select a group and then click **Configure**. The **Configuration** screen for the selected group appears.
3. From the side menu, select **Firewall**. The **Firewall Configuration** screen appears.

FIGURE 7-3. Personal Firewall – Simple Mode Screen



4. In the main frame, select the **Enable Firewall** check box.

5. Select **Simple mode**. Simple mode uses the Trend Micro recommended default settings. For more information about the default firewall settings see *Personal Firewall Defaults for Simple Mode* on page 7-9.

Tip: Trend Micro recommends uninstalling other software-based firewalls before deploying and enabling Personal Firewall. Multiple vendor firewall installations on the same computer may produce unexpected results.

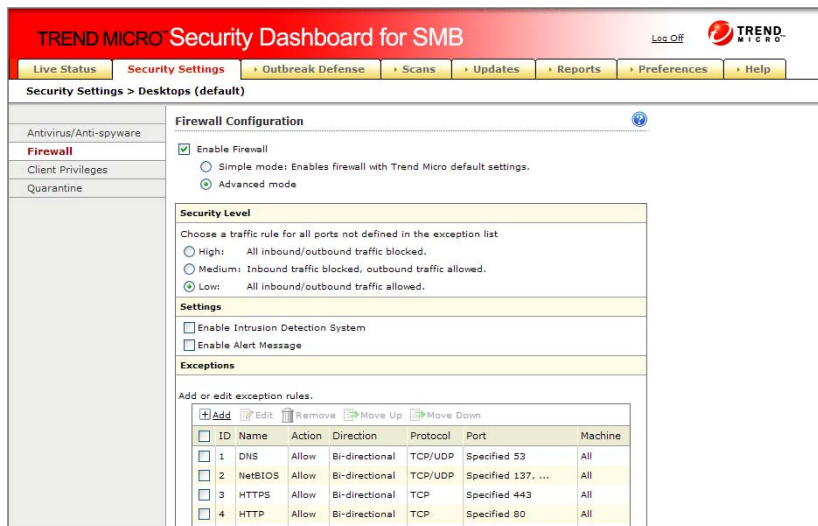
For the latest information regarding third-party firewall compatibility issues, see Knowledge Base Solution ID 20473. It is available at the following Web site:
<http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-120437>

Configuring the Personal Firewall - Advanced Mode

This section provides the necessary steps for successful deployment of Personal Firewall. By default, Client Server Security disables the Personal Firewall on all new groups and clients.

To deploy the firewall:

1. On the main menu, click **Security Settings**. The **Security Settings** screen appears.
2. Select a group or groups, and then click **Configure**. The **configuration** screen for the selected group(s) appears
3. Click **Firewall** on the side menu. The **Firewall Configuration** screen appears with **Enable Firewall** and **Simple mode** selected by default.
4. To configure advanced settings, select **Advanced mode**. The **Firewall Configuration** screen changes to display the advanced settings options.

FIGURE 7-4. Personal Firewall – Advanced Mode Screen

5. If **Enable Firewall** is not already selected, select it.
6. Under the **Security Level** heading, select a security level to allow or block inbound/outbound traffic.
7. Under the **Settings** heading, select the options to apply. The options are **Enable Intrusion Detection System** and **Enable Alert Message**.
8. Under the **Exceptions** heading, select the ports to exclude from blocking in the event of an outbreak.

To add, remove, or edit the port exception list, click the corresponding tool and follow the onscreen instructions. To create a new exception, perform the following:

- a. Click **Add**. The **Add Exception** screen appears.
- b. Type a name for the exception.
- c. Next to **Action**, choose whether to allow or deny network traffic for this exception.
- d. Next to **Direction**, select **Inbound** and/or **Outbound**.

- e. From the **Protocol** list, select a network traffic protocol:
 - All
 - TCP/UDP (default)
 - TCP
 - UDP
 - ICMP
 - f. Specify ports to exclude from blocking:
 - **All ports** (default)
 - Port range
 - **Specified ports**
 - g. Under **Machines**, specify client IP addresses.
 - **All IP addresses** (default)
 - **Single IP** – To resolve the client host name to an IP address, click **Resolve**.
 - IP range
 - h. Click **Save**. The **Firewall Configuration** screen appears with the new exception in the exception list.
9. Click the check boxes next to the exceptions you want to include.

Disabling the Firewall

From the Security Dashboard, disable Personal Firewall on client computers.

To disable the Personal Firewall:

1. On the main menu, click **Security Settings**. The **Security Settings** screen appears.
2. Select a group and then click **Configure**. The configuration screen for the selected group appears.
3. From the side menu, select **Firewall**. The **Firewall Configuration** screen appears.
4. To disable the firewall for the group, deselect the **Enable Firewall** check box.

5. Click **Save**.

Note: Deselecting the **Enable Firewall** check box will disable the firewall for both simple and advanced mode.

Using Desktop Privileges

You can grant users privileges to modify individual scan settings and remove or unload the client, while retaining control over Client Server Security on your network. Granting users privileges is simply a way of sharing control over individual client settings.

However, to enforce a uniform antivirus policy throughout your organization, Trend Micro recommends granting limited privileges to users. This ensures that Client Server Security does not modify the scan settings or remove the clients without permission.

To grant privileges to clients:

1. On the main menu, select **Security Settings**. The **Security Settings** screen appears. Select the group to which to grant privileges, and then from the **Security Settings** toolbar, click the **Configure** icon. The configuration screen for the selected group appears.
2. From the side menu, select **Client Privileges**.

FIGURE 7-5. Desktops and Servers Privileges Screen

TREND MICRO Security Dashboard for SMB [Log Off](#)

Live Status Security Settings Outbreak Defense Scans Updates Reports Preferences Help

Security Settings > Desktops (default)

Client Privileges

Grant clients the privilege to modify the following settings:

Antivirus

☐ Manual Scan settings ☐ Stop Scheduled Scan
☐ Scheduled Scan settings ☐ enable roaming mode
☐ Real-time Scan settings

Anti-spyware

☐ Manual Scan settings
☐ Scheduled Scan settings
☐ Real-time Scan settings

Firewall

☐ Display Firewall tab
☐ Allow clients to enable/disable firewall

Mail Scan

☒ Display mail scan tab
☒ Allow users to install/upgrade the POP3 mail scan module
☒ Allow users to enable/disable real-time scan for POP3 mail

Proxy Settings

☒ Allow the agent user to configure proxy settings
 (Disabling this feature will reset the proxy settings to their default)

Update Privileges

☒ Perform "Update Now!"

3. Select the privileges to grant users.

- **Antivirus**
 - Manual Scan settings
 - Scheduled Scan settings
 - Real-time Scan settings
 - Stop Scheduled Scan
 - Enable roaming mode
- **Anti-spyware**
 - Manual Scan settings
 - Scheduled Scan settings
 - Real-time Scan settings
- **Firewall**
 - Display Firewall tab
 - Allow desktops to enable/disable firewall

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

- **Mail Scan** – Select the check boxes for the Mail Scan privileges to grant users.
 - Display mail scan tab
 - Install/upgrade POP3 mail scan module
 - Real-time POP3 mail scan settings
- **Proxy Setting**
 - Allow agent user to configure proxy settings
- **Update Privileges**
 - Perform "Update Now!"
 - Enable/Disable Scheduled Update
- **Update Settings**
 - Download from Trend Micro ActiveUpdate Server

Tip: To ensure that laptop users are updated when they are out of the office, make sure that the **Download from Trend Micro ActiveUpdate Server** option is selected.

- Enable Scheduled Update
- Forbid program upgrade and hot fix deployment

When client users initiate an update, the client machine gets updates from the update source specified on the **Update Source** screen. If the update fails, the client machines attempt to update from the Trend Micro Security Server. Selecting **Download from the Trend Micro ActiveUpdate server** enables clients to attempt to update from the Trend Micro ActiveUpdate server if the update from the Trend Micro Security Server fails.
- **Client Security**

- **Normal** – Click to allow clients read/write access to the **Client/Server Security Agent** folders, files, and registries on client machines.
- **High** – Click to restrict clients from accessing **Client/Server Security Agent** folders, files, and registries.

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

4. Click **Save**.

Using Quarantine

In **Quarantine** directory, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path to store the infected files. If an invalid quarantine directory is specified, Client Server Security uses the default quarantine directory on the client:

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

To set the Quarantine directory:

1. On the main menu, click **Security Settings**. The **Security Settings** screen appears.
2. Select a desktop or server and click **Configure**. The **Configuration** screen for the selected item appears.
3. Click **Quarantine** from the side menu. The **Quarantine Directory** screen appears.

FIGURE 7-6. Desktop/Server Quarantine Screen

The screenshot displays the 'Trend Micro Security Dashboard for SMB' interface. At the top, there is a red header bar with the product name and a 'Log Off' link. Below the header is a navigation menu with tabs: 'Live Status', 'Security Settings', 'Outbreak Defense', 'Scans', 'Updates', 'Reports', 'Preferences', and 'Help'. The 'Security Settings' tab is active, and the sub-menu 'Desktops (default)' is selected. On the left side, there is a vertical menu with options: 'Antivirus/Anti-spyware', 'Firewall', 'Client Privileges', and 'Quarantine'. The 'Quarantine' option is highlighted. The main content area is titled 'Quarantine Directory' and contains a text box for specifying the quarantine directory for antivirus. The text box contains the value 'HTTP://192.168.0.13'. Below the text box, there is a small note: 'Specify a URL or a UNC path (e.g., HTTP://<CSM Server> or \\<CSM Server>\CSM\Virus)'. A 'Save' button is located at the bottom of the form.

4. In **Quarantine** directory, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path to store the infected files. If an invalid quarantine directory is specified, Client Server Security uses the default quarantine directory on the client.
5. Click **Save**.

Using Outbreak Defense

This chapter explains the Outbreak Defense Strategy, how to configure Outbreak Defense, and how to use it to protect your network and clients.

The topics discussed in this chapter include:

- *The Outbreak Defense Strategy* on page 8-2
- *Current Status* on page 8-2
- *Potential Threat* on page 8-8
- *Settings* on page 8-8
- *Using Exception* on page 8-9
- *Using Scheduled Policy Download Settings* on page 8-9

The Outbreak Defense Strategy

The Outbreak Defense Strategy is based on the idea that outbreaks have a lifecycle. They (the infection) start slow, infecting only a few clients initially. As time goes on, the few infected clients unknowingly pass the infection to other clients. At this point, the infection has spread throughout the network, or if the affect of the infection was noticeable, the client users and administrator realized they have a problem and take action. Slowly, the outbreak subsides. Maybe the infection gets chance to flare up again as unaware and unprotected client users connect to other infected clients, or open infected emails. The Outbreak Defense Strategy was designed to manage outbreaks at every point along the outbreak lifecycle.

Current Status

Displays the on-going status of your clients and network in response to a current worldwide virus outbreak. The status roughly corresponds to the outbreak lifecycle. Outbreak Defense first takes preventative measures such as informing you of the threat and taking action as prescribed in the Outbreak Prevention Policy (downloaded from TrendLabs). Next, your clients are protected from the threat when updated components are downloaded from the Trend Micro ActiveUpdate server and deployed. Finally, Damage Cleanup Services, using newly updated components, starts to clean infected and damaged files, and remove virus remnants.

FIGURE 8-1. Outbreak Defense Screen – No Threat

TREND MICRO Security Dashboard for SMB Log Off

[Live Status](#)
[Security Settings](#)
[Outbreak Defense](#)
[Scans](#)
[Updates](#)
[Reports](#)
[Preferences](#)
[Help](#)

Outbreak Defense > Current Status

Threat Prevention → Threat Protection → Threat Cleanup

Trend Micro Security Server will automatically deploy a response to a world wide virus outbreak. You will find the details of the threat and the actions that you must take below. Any action that the system cannot take automatically will be shown to you in the Vulnerable Computer(s) and Computer(s) Cleanup sections below.

Last updated: 2006/10/25 17:06:42 [Refresh](#)

Prevention

Threat Information					
Threat	Alert Type	Risk Level	Delivery Method	Vulnerability Exploited	Automatic Response
	N/A				Disable
Date/Time Initialed	Date/Time End	Automatic Response Details			
N/A	N/A	N/A			

Alert Status of your network:

Alert Status for Online Computers		
Computer Type	Enabled	Not Enabled
Desktops/Servers	N/A	N/A
Exchange servers	N/A	N/A

Threat Prevention

The Threat Prevention stage of the Current Status screen displays information about recent threats, computers that have alerts enabled, and computers that are vulnerable to the current threat.

FIGURE 8-2. Outbreak Defense Screen – Threat Prevention Stage

TREND MICRO™ Security Dashboard for SMB

Log OffTREND MICRO™

Live Status

Security Settings

Outbreak Defense

Scans

Updates

Reports

Preferences

Help

Outbreak Defense > Current Status

Threat Prevention

Threat Protection

Threat Cleanup

Trend Micro Security Server will automatically deploy a response to a world wide virus outbreak. You will find the details of the threat and the actions that you must take below. Any action that the system cannot take automatically will be shown to you in the Vulnerable Computer(s) and Computer(s) Cleanup sections below.

Last updated: 2006/10/25 16:47:35Refresh

Prevention

Red Alert Enabled

Threat TEST_MALWARE.A is currently spreading on the Internet. Trend Micro has taken action to prevent an outbreak on your network. New components will be available shortly. You can learn more about this threat by reading below.

Threat Information					
Threat	Alert Type	Risk Level	Delivery Method	Vulnerability Exploited	Automatic Response
TEST_MALWARE.A	Red Alert	Medium	Share, Email, Web, Sean Sean Sean Sean Sean Sean Sean Sean Sean Sean Sean	MS05-036	Disable
Date/Time Initialed		Date/Time End		Automatic Response Details	
2006/10/25 16:46:06		2006/10/27 16:46:06		View...	
*** Testing No.300 *** From CSM QA,this message will show on threat info. Using VA pattern version 1. Require Virus Pattern. Testing for TEST_MALWARE.A with a fake IO MS05-036 (modified, for testing). Need TMVAINFO.xml to create a fake to support and using special tsc.exe, tsc.pth					

Threat Information

The Threat Information section displays information about viruses that are currently on the Internet and that could potentially affect your network and clients. Threat Information, using the Outbreak Prevention Policy, takes steps to protect your network and clients while TrendLabs develops a solution (See *Trend Micro Outbreak Prevention Policy* on page B-1).

Threat Information

This panel displays the name of the current outbreak threat. Learn more about this threat by clicking **Help > Security Info** to redirect your browser to the Trend Micro Web site.

- **Risk Level**—the level of risk the threat poses to computers and networks based on the number and severity of virus and malware incident
- **Automatic Response Details**—click to view the specific actions Outbreak Defense is using to protect your computers from the current threat. Click **Disable** to stop the Automatic Response from the server-side. Stopping the Automatic Response on the server-side will stop it for the Client/Server Security Agents as well.

Alert Status for Online Computers

The Alert Status for Online Computers displays a total for the number of clients that do and do not have automatic alert enabled. Click the number link under the **Enabled** and **Not Enabled** columns to view more information about specific client computers.

Vulnerable Computer(s)

The Vulnerable Computer(s) section displays a list of clients that have vulnerabilities that make them susceptible to the threat displayed in the Threat Information section.

Threat Protection

The Threat Protection stage of the Current Status screen provides information about the components that are affected by the threat, and the solution download and deployment status.

FIGURE 8-3. Outbreak Defense Screen – Protection Stage

TREND MICRO Security Dashboard for SMB Log Off

Live Status Security Settings **Outbreak Defense** Scans Updates Reports Preferences Help

Outbreak Defense > Current Status

Threat Prevention → Threat Protection → Threat Cleanup

Trend Micro Security Server will automatically deploy a response to a world wide virus outbreak. You will find the details of the threat and the actions that you must take below. Any action that the system cannot take automatically will be shown to you in the Vulnerable Computer(s) and Computer(s) Cleanup sections below.

Last updated: 2006/10/25 15:44:15

Prevention Red Alert Enabled

Protection for TEST_MALWARE.A

Solution Download Status		
Component	Version	Status
Virus cleanup template	999	Not downloaded yet
Virus cleanup engine 32-bit	3.980.0000	Downloaded
Virus pattern	3.297.00	Downloaded

Solution Deployment Status		
Computer Type	Up-to-date	Out-of-date
Desktop/Server	2	3
Exchange server	1	0

Solution Download Status

Displays a list of components that need to be updated in response to the threat listed in the Threat Information section.

Solution Deployment Status

Displays the number of clients that have Up-to-date components. Displays the number of clients that have out-of-date components. Provides a link to view clients with up-to-date or out-of-date components.

Threat Cleanup

The Threat Cleanup stage of the Current Status screen displays the status of the scan that takes place after the updated components have been deployed. The Cleanup section also displays the status of computers after the scan, and lists whether the updates were successful in cleaning or removing threat remnants.

FIGURE 8-4. Outbreak Defense Screen - Cleanup Stage

TREND MICRO Security Dashboard for SMB Log Off

Live Status Security Settings **Outbreak Defense** Scans Updates Reports Preferences Help

Outbreak Defense > Current Status

Threat Prevention → Threat Protection → Threat Cleanup

Trend Micro Security Server will automatically deploy a response to a world wide virus outbreak. You will find the details of the threat and the actions that you must take below. Any action that the system cannot take automatically will be shown to you in the Vulnerable Computer(s) and Computer(s) Cleanup sections below.

Last updated: 2006/10/25 15:59:31

☒ Prevention Red Alert Enabled

☒ Protection for TEST_MALWARE.A

☒ Cleanup for TEST_MALWARE.A

Security Server has scanned your network with the latest threat solution. See a list of computers that are scanned below.

Computer Scanning Status for TEST_MALWARE.A		
Computer Type	Scanned	Not Scanned
Desktop/Server	0	2
Exchange server	0	1

Security Server has scanned your network with the latest threat solution. See a list of computers that are scanned below.

Computer Cleanup Status for TEST_MALWARE.A					
Attempts/total: 4/7					
Export					
Total: 1 Record(s) 1 of 1					
Computer	Date/Time	IP Address	Computer Group	Threat Name	Cleanup Result
C-B-8	2006/10/25 16:49:14	10.5.0.108	Servers (default)	TEST_MALWARE.A	Cleaned successfully

Note: For a scan to automatically take place after the new components have been deployed, it has to be enabled in the Outbreak Defense > Settings screen.

Computer Scanning Status for

Click the links to display a list of Client computers that have received notification to scan for threats or that have not yet received notification. Client computers that are not turned on or that have been disconnected from the network cannot receive notifications.

Computer Cleanup Status for

This panel displays the results of the Cleanup scan.

Potential Threat

The Potential Threat screen uses the information gathered from Vulnerability Assessment and Damage Cleanup Services to display information about clients that, because they are already infected or have vulnerabilities, are Potential Threats to the security of your network. Vulnerability Assessment determines which clients have vulnerabilities and Damage Cleanup Services determines which clients are still infected and need to be cleaned in order to make them safe.

Vulnerable Computer(s)

The Vulnerable Computer(s) section displays a list of clients that have vulnerabilities that make them susceptible to the most recent threat. Client Server Security uses Vulnerability Assessment to determine which clients have vulnerabilities. To learn more about Vulnerability Assessment see [Vulnerability Assessment](#) on page B-3.

Computer(s) to Cleanup

The Computer(s) to Cleanup section displays information about infected computers. Administrators can also perform a real-time cleanup of infected computers using updated cleanup security components. The Cleanup service uses Trend Micro Damage Cleanup Services. To learn more about how Damage Cleanup works, see [Trend Micro Damage Cleanup Services](#) on page B-2.

To perform a real-time cleanup of infected computers using newly updated cleanup components:

1. Click **Cleanup Now** in the **Threat Cleanup** table.
2. A **Threat Cleanup** progress bar appears displaying the progress of the threat cleanup process.
3. After the cleanup process is completed, a **Cleanup Notifying Results** screen appears.

Settings

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

Outbreak Defense

Use Outbreak Defense to configure threat response settings, block or unblock ports, and schedule when and how often the Outbreak Prevention Policy is updated.

Note: After you disable Outbreak Defense, Trend Micro recommends running Cleanup Now to help rid your clients of Trojans and any running processes related to Trojans, or other types of malicious code (see *Computer(s) to Cleanup* on page 8-8).

Using Exception

Use Exception to Add new ports to, and Edit or Remove existing ports from the list of ports to exclude from blocking.

Note: When adding a new exception, make sure that **Enable this exception** is checked.

Using Scheduled Policy Download Settings

Use Scheduled Policy Downloads to set when and how often the Security Server checks for and downloads new Outbreak Prevention Policies. By default, the Security Server checks for new Outbreak Prevention Policies every 30 minutes and downloads new policies as required.

To set a Scheduled Policy Download source and time:

1. From the main menu, click **Outbreak Defense > Settings**. The Settings screen appears. The **Outbreak Defense** tab is selected by default.
2. Click the plus (+) icon for the **Scheduled Policy Download Settings** section.
3. From the **Scheduled Policy Download Settings** section, set the following options:
 - a. **Frequency:** The default time is every 30 minutes.
 - b. **Source:** Choose from where to download updates. The default is the Trend Micro ActiveUpdate server:
 - Trend Micro ActiveUpdate server
 - Intranet location containing a copy of the current file

- Other update source
4. Click **Save**.

Vulnerability Assessment

To set a time for Vulnerability Assessment:

1. Click **Outbreak Defense > Settings** to open the Settings screen.
2. Click the **Vulnerability Assessment** tab.
3. Select **Enable Scheduled Vulnerability Prevention**
4. Set the schedule using the following options (applies to all clients):
 - **Daily** – Click to perform a vulnerability assessment every day
 - **Weekly, every** – Click to perform a vulnerability assessment once a week.
You must select a day from the list and a start time. The time selected is the time that Client Server Security will perform the scan.
 - **Monthly, on day** – Click to perform a vulnerability assessment once a month.
You must select a date from the list and a start time.

Regardless of the selection, specify when to start vulnerability assessment in the **Start time** lists.

5. Set the **Target** for the scan.
 - Select **All groups** to scan all the computers that appear in the Group Management Tree on the Security Settings screen.
 - Select the **Specified group(s)** to limit the vulnerability assessment scan to only the specific groups you designate.
6. Click **Save**.

Manual and Scheduled Scans

This chapter describes Manual and Scheduled scans and how to use Manual and Scheduled scan to protect your network and clients from viruses, malware, and other threats.

The topics discussed in this chapter include:

- *Manual and Scheduled Scans* on page 9-2
- *Scanning Desktops and Servers for Viruses, Spyware, and Other Malware Threats* on page 9-2

Manual and Scheduled Scans

Client Server Security provides three types of scans to protect your clients from viruses, malware, and other types of malicious code: Manual Scan, Scheduled Scan, and Real-time Scan. Each scan has a different purpose and use, but all are configured approximately the same way. This chapter discusses Manual and Scheduled Scans.

About Scans for Desktops and Servers

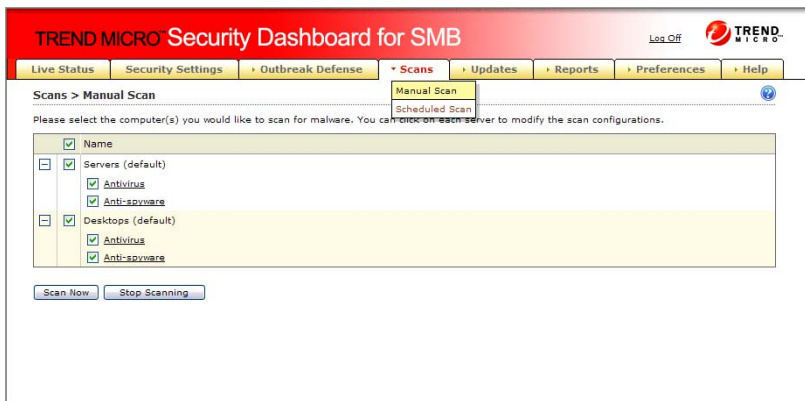
Manual Scan – Occurs after user execution and completely scans all specified files. The length of the scan depends on the number of files and your hardware resources.

Scheduled Scan – A scheduled scan completely scans all files at the time and frequency configured. Use scheduled scans to automate routine scans on your clients and improve virus management efficiency.

Scanning Desktops and Servers for Viruses, Spyware, and Other Malware Threats

Because creating Manual and Scheduled Scans for desktops and servers are similar, the steps for configuring the two will be combined. An additional section for setting a scan schedule will follow.

FIGURE 9-1. Manual Scan Screen



To configure Manual or Scheduled Scans for desktops and servers:

1. Click **Scans > Manual Scan** or **Scheduled Scan** to open the Scan screen.
2. Select the group(s) to scan.
3. Optional: Set the antivirus and anti-spyware scanning options by clicking the group name, and then clicking either **Antivirus** or **Anti-spyware**.

Anti-spyware Settings

- a. Verify that the **Anti-spyware** check box is selected for each group.
 - b. To configure the anti-spyware scan settings, click the **Anti-spyware** link. The manual anti-spyware scan settings page appears.
 - c. On the **Target** tab, select the type of anti-spyware scan to run. Available options include:
 - Full scan – Scans the entire disk and registry for spyware
 - Quick scan – Examines common areas where spyware is typically installed
 - d. On the **Action** tab, click an action to perform on any spyware that is detected. Available options include:
 - Clean – Remove the spyware from infected clients
 - Pass – Only record the detected spyware in the spyware logs
 - e. Click **Save** to save your scan settings, and then **Back** to go back to the Scan Now page.
4. Click **Scan Now** to run a Manual Scan or click **Save** to save the Scheduled Scan settings.

To set a time for Scheduled scans:

1. Click **Scans > Scheduled Scan** to open the Scheduled Scan screen.
2. Click the **Schedule** tab. A table displaying a list of all scannable clients appears.
3. For each client create a schedule using the following UI elements:
 - **Daily** – Click to perform Scheduled Scan every day
 - **Weekly, every** – Click to perform a Scheduled Scan once a week. You must select a day from the list and a start time. The time selected is the time that Client Server Security will perform the scan.

- **Monthly, on day** – Click to perform a Scheduled Scan once a month. You must select a date from the list and a start time.

Regardless of the selection, specify when to start scheduled scans in the **Start time** lists.

4. Click **Save.**

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

Note: To disable Scheduled Scan, deselect all options for the specific desktops and servers and click **Save**.

Tip: Trend Micro recommends that you set Client Server Security to run scheduled scans at regular intervals for optimal protection of your desktops and servers.

Updating Components

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

The topics discussed in this chapter include:

- *Choosing an Update Source* on page 10-2
- *Updating the Components* on page 10-3
- *Updating the Trend Micro Security Server* on page 10-4
- *Manual and Scheduled Updates* on page 10-4
- *Setting the Update Source for the Trend Micro Security Server* on page 10-6
- *Default Update Times* on page 10-7
- *Using Update Agents* on page 10-8
- *Rolling Back Components* on page 10-10

Choosing an Update Source

When choosing the location(s) from where to update clients, consider the bandwidth of the sections of your network that are between clients and the update source(s). The following table describes different component update options and recommends when to use them:

TABLE 10-1. Update Source Options

Update Option	Description	Recommendation
ActiveUpdate server > Trend Micro Security Server > clients.	The Trend Micro Security Server receives updated components from the ActiveUpdate server (or other update source) and deploys them directly to clients.	Use this method if there are no sections of your network between the Trend Micro Security Server and clients you identify as 'low-bandwidth'.
ActiveUpdate server > Trend Micro Security Server > Update Agents > clients	The Trend Micro Security Server receives updated components from the ActiveUpdate server (or other update source) and deploys them directly to Update Agents, which deploy the components to clients.	Use this method to balance the traffic load on your network if there are sections of your network between the Trend Micro Security Server and clients you identify as 'low-bandwidth'.
ActiveUpdate server > Update Agents > clients	Update Agents receive updated components directly from the ActiveUpdate server (or other update source) and deploy them to clients.	Use this method only if you are experiencing problems updating Update Agents from the Trend Micro Security Server or from other Update Agents. Under most circumstances, Update Agents receive updates faster from the Trend Micro Security Server or from other Update Agents than from an external update source.

Updating the Components

To ensure that your clients stay protected from the latest virus threats and other malicious code, you need to update the Client Server Security components regularly. To view details about the components that Client Server Security uses to protect your clients see [Client Server Security Updateable Components](#) on page 2-5.

Configure the Trend Micro Security Server to download Client Server Security components from the Trend Micro ActiveUpdate server. After the server downloads any available updates, it automatically deploys these to the clients.

Client Server Security provides two methods for updating your components:

- Update your components manually
- Update your components based on a schedule

For information on how to update your components, see [To update the Trend Micro Security Server components](#): on page 10-5.

For information on how to set a schedule for updates, see [To set a schedule to check for updated components](#): on page 10-6.

If you use a proxy server to connect to the Internet, make sure you properly configure your proxy settings to download updates successfully. For information on how to configure your proxy settings, see [Internet Proxy Options](#) on page 13-1.

TABLE 10-2. Updatable Components

Component	Sub-component
Antivirus	• Virus pattern • Virus scan engine 32-bit • Virus scan engine 64-bit • Virus cleanup template • Virus cleanup engine 32-bit • IntelliTrap exception pattern • IntelliTrap pattern
Anti-spyware	• Spyware scan engine 32-bit • Spyware scan engine 64-bit • Spyware pattern • Spyware active-monitoring pattern • Anti-rootkit driver 32-bit
Outbreak Defense	• Vulnerability pattern

TABLE 10-2. Updatable Components

Component	Sub-component
Network Virus	• Common firewall pattern • Common firewall engine 32-bit

Updating the Trend Micro Security Server

To help ensure that computers and servers on your network stay protected against the latest threats, regularly update the Client Server Security components.

Do the following to configure Trend Micro Security Server to perform updates:

1. Configure the Trend Micro Security Server for manual or scheduled updates.
2. Select an update source.
3. Use Desktop Privileges to configure update options for clients running the Client/Server Security Agent and/or the Messaging Security Agent.

Manual and Scheduled Updates

Manual Updates

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

Scheduled Updates

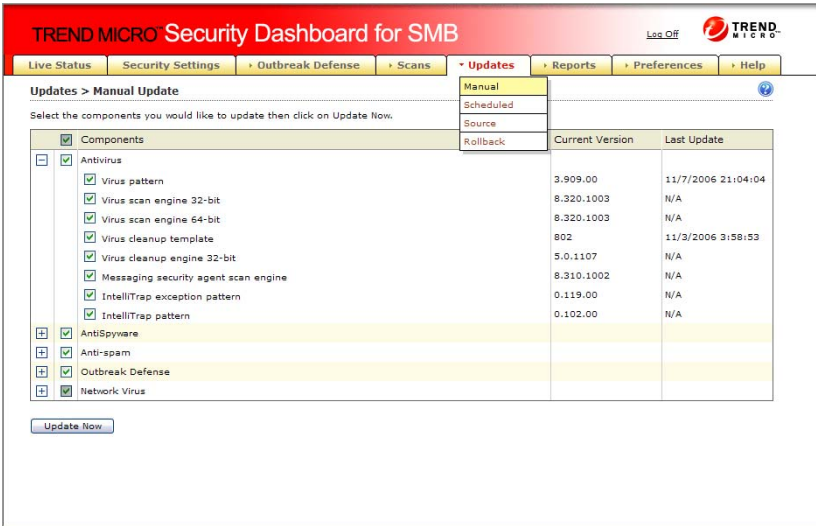
Configure the Trend Micro Security Server to regularly check its update source and automatically download any available updates. Because clients normally get updates from the Trend Micro Security Server, using automatic scheduled update is an easy and effective way of ensuring that your protection against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

Note: As soon as the Trend Micro Security Server receives updated components, they are automatically deployed to clients.

To update the Trend Micro Security Server components:

1. On the main menu, click **Updates > Manual** or **Scheduled**. The **Update** screen appears.

FIGURE 10-1. Manual Update Screen



2. Under components section, select the components to update.
To update all components, select the **Components** check box.
3. Click **Update Now** to Manually update the components, or click **Save** if setting a Scheduled update.

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

To set a schedule to check for updated components:

1. Click **Updates > Scheduled** to open the Scheduled Update screen.
2. Click the **Schedule** tab.
3. For each client create a schedule using the following UI elements:
 - **Hourly** – Click to perform an update every hour
 - **Daily** – Click to perform an update every day
 - **Weekly, every** – Click to perform an update once a week. You must select a day from the list and a start time. The time selected is the time that Client Server Security will check for and download updated components.
 - **Monthly, on day** – Click to perform an update once a month. You must select a date from the list and a start time.

Regardless of the selection, specify when to start scheduled updates in the **Start time** lists.

4. Click **Save**.

Setting the Update Source for the Trend Micro Security Server

Choose from where and how Trend Micro Security Server receives its updates.

Set up an update source for the Trend Micro Security Server:

1. From the main menu, click **Updates > Source**. The **Update Source** screen appears.

FIGURE 10-2. Update Source Screen

2. From the **Download updates from** section, choose from where to download updates:
 - Trend Micro ActiveUpdate server
 - An intranet location containing a copy of the current file
 - An other update source.
3. Click **Save**.

Default Update Times

By default Client Server Security downloads components from the Trend Micro ActiveUpdate server under the following circumstances:

- When you install the product for the first time, all of components for the Security Server and client computers are immediately updated from the Trend Micro ActiveUpdate server.
- Whenever the Client Server Security master service is started, the Security Server updates the Outbreak Defense policy.
- By default, Scheduled Updates run every hour to update the Security Server.

- To ensure that client computers stay up-to-date, Client Server Security Agent runs a scheduled update for the client computers every 8 hours.

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

Trend Micro updates the scan engine or program generally only during the release of a new Client Server Security version. However, Trend Micro releases pattern files every day to keep your client virus protection current.

Using Update Agents

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

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

To allow one or more CSAs to act as Update Agents:

1. On the main menu, click **Updates > Source**. The update source screen appears.
2. Click the **Security Agents** tab.
3. Under the Assign Update Agent(s) section, click **Add**. The Add an Update Agent screen appears.
4. From the **Select Security Agent(s)...** list box, select one or more CSAs to act as Update Agents.
5. Click **Save**.

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

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

1. On the main menu, click **Updates > Source**. The update source screen appears.

2. Click the **Security Agents** tab.
3. Under the Alternative Update Source section, select **Enable Alternative Update Sources**.
4. [Optional]—Select **Always update from Security Server for Update Agents**.

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

5. Click **Add**. The Add an Alternative Update Source screen appears.
6. Enter a range of IP addresses. CSAs with IP addresses that fall within this range will receive their updates from the update source you specify:
 - a. **IP from**—Type the first IP address in the range.
 - b. **IP to**—Type the last IP address in the range.

Note: To specify a single CSA, enter the CSA IP address in both the **IP from** and **IP to** fields.

7. Select an update source:
 - **Update Agent**—Select an Update Agent as a source for updates.
- or -
 - **Specified**—Specify a path to an update source.
8. Click **Save**.

Note: CSAs not specified will automatically receive their updates from the Trend Micro Security Server.

To stop CSAs from acting as Update Agents:

1. On the main menu, click **Updates > Source**. The update source screen appears.
2. Click the **Security Agents** tab.

3. Under the Computer Name column, select the CSAs that you no longer wish to act as Update Agents.
4. Click **Remove**.

To stop CSAs from receiving updates from alternative update sources:

1. On the main menu, click **Updates > Source**. The update source screen appears.
2. Click the **Security Agents** tab.
3. Under the IP Range column, select one or more of the IP address range(s).
4. Click **Remove**.

Rolling Back Components

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

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

The Security Server uses the following scan engines:

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

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

To roll back the pattern file or scan engine:

1. On the menu, click **Updates > Rollback**. The Rollback screen appears showing the current versions of your virus pattern file and scan engine, and the previous versions of these components, if any.
2. Click **Synchronize with Server** under the appropriate section.
3. Click **Back** to return to the original Rollback screen.

4. If an older version pattern file exists on the server, you can roll back both the client and the server. Click **Rollback server and agents**. The Rollback screen appears.

Viewing and Interpreting Logs

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

The topics discussed in this chapter include:

- *Viewing and Interpreting Logs* on page 11-2
- *Management Console Event Logs* on page 11-2
- *Desktop/Server Logs* on page 11-2
- *Using Log Query* on page 11-3
- *Creating One-time Reports* on page 11-5
- *Deleting One-time Reports* on page 11-6
- *Scheduling Reports* on page 11-6
- *Deleting Scheduled Reports* on page 11-7
- *Editing Scheduled Reports* on page 11-8
- *Maintaining Logs and Reports* on page 11-9

Viewing and Interpreting Logs

Client Server Security keeps comprehensive logs about virus and spyware incidents, events, and updates. This section contains a list of the different logs. Use these logs to assess your organization's virus protection policies and to identify clients that are at a higher risk of infection. Also, use these logs to verify that updates have been deployed successfully.

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

Client Server Security maintains logs under the following categories:

- Management console event logs
- Desktop/Server logs

Management Console Event Logs

Each type of log contains different information.

- Manual scan log
- Update log
- Outbreak Defense event log
- Console event log

Desktop/Server Logs

- Virus log
- Spyware log
- Update log
- Network virus log
- Outbreak Defense log
- Event log

Using Log Query

This section describes how to use the Log Query screen to view log information.

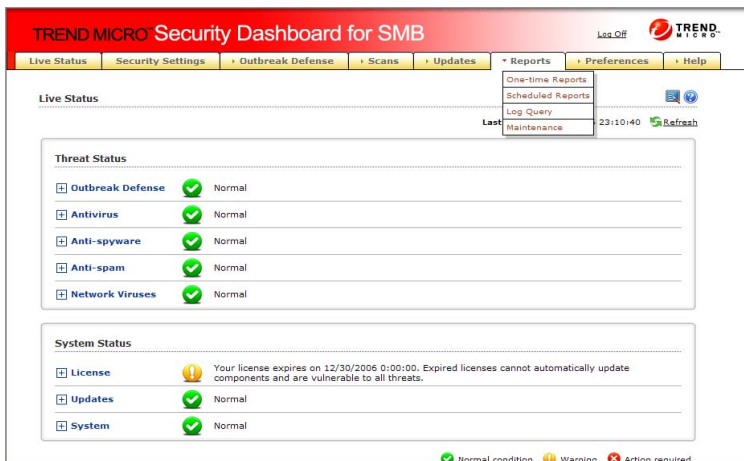
TABLE 11-1. Log Type and Content

Type (event or item that generated the log entry)	Content (type of log to obtain content from)
Management console events	• Manual scan • Update • Outbreak Defense events • Console events
Desktop/Server	• Virus logs • Manual scan • Real-time scan • Scheduled scan • DCS scan • Spyware logs • Manual scan • Real-time scan • Scheduled scan • Update logs • Network virus logs • Outbreak Defense logs • Event logs

Client Server Security records log entries for many different events. Use log query to view the different logs.

To view virus logs:

1. On the main menu, click **Reports > Log Query**. The **Log Query** screen appears.

FIGURE 11-1. Default Log Query Screen

2. Under **Time Range**, select **All dates** or select **Specified range** and type a range of dates.
3. Under **Type**, select from one of the following:
 - **Management console events**
 - **Desktop/Server**

Note: The items displayed in the **Content** list will depend on the **Type** selected

4. Under **Content**, select the type of log to view.
5. To view the log, click **Display Logs**. The appropriate log screen appears.
6. To save the log as a comma-separated value (CSV) data file, click **Export**. Use a spreadsheet application to view CSV data files.

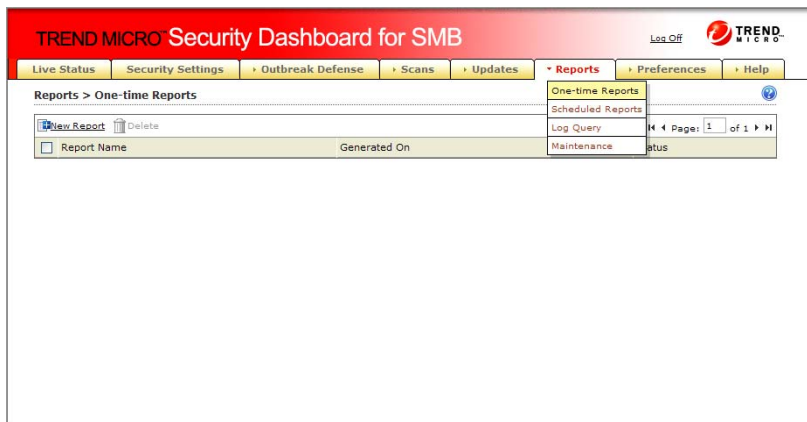
Creating One-time Reports

This section describes how to create a one-time report.

To create a one-time report:

1. From the main menu, click **Reports > One-time Reports**, the **One-time Reports** screen appears. From the One-time reports toolbar, click **New Report** icon, the **New Report** screen appears.

FIGURE 11-2. Create One-time Report Screen



2. Type a report name in the **Report name** text box.
3. Under the **Time Range** section, type the dates in the **From** and **To** that you want the report to include.
4. Under the **Content** section, to create a report that lists all the different Threat events, select the **Select All** check box. To receive information on specific threats, select the appropriate check box.
5. Under the **Send Report** section, select the **Send report to** check box, and then type the email addresses to which you want to send the report.
6. Click **Generate**.

Deleting One-time Reports

This section describes how to delete a One-time report.

To delete a One-time report:

1. From the main menu, click **Reports > One-time Reports**, the **One-time Reports** screen appears.
2. Select the report to be deleted.
3. From the One-time reports toolbar, click the **Delete** icon, a message box will appear, verifying the request to delete the report.
4. Click **Yes**. The report no longer appears in the One-time report screen.

Scheduling Reports

This section describes how to create reports using the Scheduled report screen.

To schedule reports:

1. From the main menu, click **Reports > Scheduled Reports**, the **Scheduled Reports** screen appears. From the Scheduled reports toolbar, click **Add**. The **Add a report template** screen appears.

FIGURE 11-3. Create Scheduled Report Screen

TREND MICRO Security Dashboard for SMB Log Off

Live Status | Security Settings | Outbreak Defense | Scans | Updates | **Reports** | Preferences | Help

Reports > Scheduled Reports > Add a report template

Report template name:

Schedule

☒ Daily
☐ Weekly, every
☐ Monthly, on day
Generate report at: : (hh:mm)

Content ☐ Select all

☐ Antivirus
☐ Outbreak Defense History
☐ Anti-spyware
☐ Anti-spam summary
☐ Content Filtering
☐ Network Virus

Send Report

☐ Send the report to:
Separate multiple entries with a semicolon (;)
Example: user1@domain.com; user2@domain.com

☒ As a PDF attachment
☐ As a link to the report

2. Enter a report name in the **Report name** text box.
3. Under the **Schedule** section, select **Daily** to create a report on a daily basis, or choose **Weekly** and select a day of the week to generate the report. Select **Monthly** and enter a day of the month to generate the report on a monthly basis. For daily, weekly, and monthly reports, the time of day to generate must be selected.
4. Under the **Content** section, to create a report that lists all the different Threat events, select the **Select All** check box. To receive information on specific threats, select the appropriate check box.
5. Under the **Send Report** section, select the **Send report to** check box, and then type the email addresses to which you want to send the report.
6. Click **Add**.

Deleting Scheduled Reports

This section describes how to delete a Scheduled report.

To delete a Scheduled report:

1. From the main menu, click **Reports > Scheduled Reports**, the **Scheduled Reports** screen appears.
2. Select the report(s) to be deleted.
3. From the Scheduled reports toolbar, click **Delete**. A message box will appear, verifying the request to delete the report.
4. Click **Yes**. The report no longer appears in the Scheduled Report screen.

Editing Scheduled Reports

This section describes how to edit a Scheduled report.

To edit a Scheduled report:

1. From the main menu, click **Reports > Scheduled Reports**, the **Scheduled Reports** screen appears.
2. Select the report(s) to be edited.
3. From the Scheduled reports toolbar, click the name of the report. The **Edit Report Settings** screen appears.
4. Select **Enable this report** if not already selected.
5. Enter a report name in the **Report name** text box.
6. Under the **Schedule** section, select **Daily** to create a report on a daily basis, or choose **Weekly** and select a day of the week to generate the report. Select **Monthly** and enter a day of the month to generate the report on a monthly basis. For daily, weekly, and monthly reports, the time of day to generate must be selected.
7. Under the **Content** section, to create a report that lists all the different Threat events, select the **Select All** check box. To receive information on specific threats, select the appropriate check box.
8. Under the **Send Report** section, select the **Send report to** check box, and then type the email addresses to which you want to send the report.
9. Click **Save**.

Maintaining Logs and Reports

This section describes how to maintain Logs and Reports using the Maintenance screen.

Maintenance - Reports

To conserve disk space on the server, specify the maximum number of reports to keep.

To set the maximum number of reports to keep:

1. On the main menu, click **Reports > Maintenance**. The **Maintenance** screen appears.

FIGURE 11-4. Reports Maintenance Screen

TREND MICRO Security Dashboard for SMB

Log Off TREND MICRO

Live Status Security Settings Outbreak Defense Scans Updates Reports Preferences Help

Reports > Maintenance

One-time Reports
Scheduled Reports
Log Query
Maintenance

Reports Auto Log Deletion Manual Log Deletion

Specify the maximum number of reports to keep.

Report Type	Maximum Reports to Keep (1-100)
One-time reports	10
Scheduled reports saved in each template	10
Report templates	10

Save

2. Select the **Reports** tab, the main body changes to display the **Reports > Maintenance** screen.
3. Under **Maximum Reports to Keep**, enter a number between 1 and 100 for each type of report listed.
4. Click **Save**.

Maintenance - Logs

To conserve disk space on the server, delete logs manually or schedule regular deletion times.

To set up auto log deletion:

1. On the main menu, click **Reports > Maintenance**. The **Maintenance** screen appears.
2. Select **Auto Log Deletion**. The Auto Log Deletions options appear.

FIGURE 11-5. Auto Log Deletion Screen

TREND MICRO Security Dashboard for SMB Log Off

Live Status Security Settings Outbreak Defense Scans Updates **Reports** Preferences Help

Reports > Maintenance

Reports **Auto Log Deletion** Manual Log Deletion

Setup criteria for deleting older logs automatically.
Note: Generated reports get information from logs. Deleting logs may delete information required by reports.

Security Server			
Log Type	First Log Entry	Most Recent Log Entry	Delete Logs Older Than
☒ Manual scan logs	N/A	N/A	30 days
☒ Update logs	11/3/2006 3:56:55	11/4/2006 4:01:35	30 days
☒ Outbreak Defense logs	N/A	N/A	30 days
☒ Console events logs	11/3/2006 3:56:44	11/5/2006 5:00:25	30 days

Desktops/Servers			
Log Type	First Log Entry	Most Recent Log Entry	Delete Logs Older Than
☒ Virus logs	N/A	N/A	30 days
☒ Spyware/Grayware logs	N/A	N/A	30 days
☒ Update logs	11/4/2006 0:23:09	11/5/2006 20:44:55	30 days
☒ Network virus logs	N/A	N/A	30 days
☒ Outbreak Defense logs	N/A	N/A	30 days
☒ Event logs	N/A	N/A	30 days

Exchange Server(s)			
Log Type	First Log Entry	Most Recent Log Entry	Delete Logs Older Than
☒ Virus logs	N/A	N/A	30 days
☒ Attachment blocking logs	N/A	N/A	30 days
☒ Content filtering logs	N/A	N/A	30 days

3. Under **Log Type**, select the types of logs to delete.
4. Under the **Delete Logs Older Than** column, type a value for number of days after which time Client Server Security or Client Server Security will delete the specified log.
5. Click **Save** to save the auto log deletion options.

To delete logs manually:

1. On the main menu, click **Reports > Maintenance**. The **Maintenance** screen appears.
2. Select **Manual Log Deletion**. The Manual Log Deletion options appear.

FIGURE 11-6. Manual Log Deletion Screen

TREND MICRO Security Dashboard for SMB Log Off

Live Status Security Settings Outbreak Defense Scans Updates **Reports** Preferences Help

Reports > Maintenance

Reports Auto Log Deletion **Manual Log Deletion**

Setup criteria for deleting older logs immediately.
Note: Generated reports get information from logs. Deleting logs may delete information required by reports.

Security Server

Log Type	First Log Entry	Most Recent Log Entry	Delete Logs Older Than
Manual scan logs	N/A	N/A	30 days Delete
Update logs	11/3/2006 3:56:55	11/4/2006 4:01:35	30 days Delete
Outbreak Defense logs	N/A	N/A	30 days Delete
Console events logs	11/3/2006 3:56:44	11/3/2006 5:00:25	30 days Delete

Desktops/Servers

Log Type	First Log Entry	Most Recent Log Entry	Delete Logs Older Than
Virus logs	N/A	N/A	30 days Delete
Spyware/Grayware logs	N/A	N/A	30 days Delete
Update logs	11/4/2006 0:23:09	11/3/2006 20:44:55	30 days Delete
Network virus logs	N/A	N/A	30 days Delete
Outbreak Defense logs	N/A	N/A	30 days Delete
Event logs	N/A	N/A	30 days Delete

Exchange Server(s)

Log Type	First Log Entry	Most Recent Log Entry	Delete Logs Older Than
Virus logs	N/A	N/A	30 days Delete
Attachment blocking logs	N/A	N/A	30 days Delete
Content filtering logs	N/A	N/A	30 days Delete

3. Under the **Delete Logs Older Than** column, type a value for number of days after which time Trend Micro Security Server will delete the specified log.
4. Click **Delete** to delete the selected log immediately.
5. Click **Save** to save the manual log deletion options.

Working with Notifications

When Client Server Messaging Security logs a significant threat or system event, it displays the results in the Live Status screen. You can set Client Server Messaging Security to send Notifications whenever these events happen. In addition, you can customize the parameters that trigger both notification and the Live Status display.

The topics discussed in this chapter include:

- *Configuring Event Notifications* on page 12-2
- *Event Types* on page 12-2
- *Notification Method Settings* on page 12-4

Configuring Event Notifications

Send notifications to yourself or other administrators in your organization whenever Client Server Security detects that any of the following events have taken place.

Event Types

Threat Events:

- **Outbreak Defense** – An alert activated, or highly critical vulnerabilities detected
- **Antivirus** – Viruses detected on clients, servers, or Exchange server exceeds a certain number, actions taken against viruses are unsuccessful, Real-time scan disabled on clients, servers, or Exchange server
- **Anti-spyware** – Spyware detected on clients and servers, including those that required the infected client to be restarted to completely remove the spyware threat. You can also configure the spyware notification threshold, that is, the number of spyware incidents detected within the specified time period (default is one hour).
- **Network Virus** – Network viruses detected exceeds a certain number

System Events:

- **License** – Product license expires, seat count usage more than 80%, or seat count usage more than 100%
- **Component update** – Last time components updated exceeds a certain number of days or updated components not deployed to clients quick enough
- **Unusual system events** – Disk space reaching dangerously low levels

To have the Security Server send notifications for the different events, do the following:

1. On the main menu, click **Preferences > Notifications**. The **Notifications** screen appears.

FIGURE 12-1. Notifications – Events Screen

TREND MICRO Security Dashboard for SMB [Log Off](#)

[Live Status](#) [Security Settings](#) [Outbreak Defense](#) [Scans](#) [Updates](#) [Reports](#) **[Preferences](#)** [Help](#)

Preferences > Notifications

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

Events [Settings](#)

Threat Events

☒ Type

☐ Outbreak Defense

☐ Antivirus

☐ Anti-spyware

☐ Anti-spam

☐ Network Virus

System Events

☒ Type

☐ License

☐ Component update

☐ System unusual events

[Save](#)

Note: The **Anti-spam** option will only appear if Client Server Security is installed.

- To receive notification of any threat event occurrence, select the **Type** check box under the **Threat Events** section.

To receive notification of specific threat event occurrences, select any of the following:

- **Outbreak Defense**
- **Antivirus**
- **Anti-spyware**
- **Anti-spam**
- **Network Virus**

- To receive notification of any system event occurrences, select the **Type** check box under the **System Events** section. The possible system events are:

- **License expiration**
- **Component update**
- **System unusual events**

4. Click **Save**.

Notification Method Settings

To ensure that recipients receive the notifications, Client Server Security provides multiple options for sending notifications. Send notifications using the following methods:

- **Email**
- **SNMP trap**
- **Windows Event Log**

To configure the different notification sending options:

1. On the main menu, click **Preferences > Notifications**. Click the **Settings** tab. The main frame changes to display the different notification sending options.

FIGURE 12-2. Notification – Schedule Screen

TREND MICRO Security Dashboard for SMB [Log Off](#)

[Live Status](#) [Security Settings](#) [Outbreak Defense](#) [Scans](#) [Updates](#) [Reports](#) [Preferences](#) [Help](#)

Preferences > Notifications

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

[Events](#) [Settings](#)

Email Notification

From: Administrator@TrendMicroCS.Local

To: admin@company.com
use semicolon ";" to separate multiple addresses
For example: user1@domain.com;user2@domain.com

SNMP Notification Recipient

☐ Enable SNMP notifications ⓘ

IP Address:

Community:

Logging

☐ Write to Windows event log

[Save](#)

To send notifications using email:

1. Under Email Notification, in the **From** field, type the email address of the Security Server.
2. Under Email Notification, in the **To** field, type the email address(es) of notification recipients. Separate multiple email addresses with a semicolon.
3. Click **Save**.

To send notifications using SNMP Notification:

1. Select **Enable SNMP Notifications**
2. Type the IP address for SNMP trap notifications and the community name.
3. Click **Save**.

To send notifications using the Windows event log:

1. Select the **Write to Windows event log** check box.
2. Click **Save** to save the settings.

Note: Use one or all of the previous methods to send notifications

Configuring Global Settings

This chapter explains how to use Global Settings.

The topics discussed in this chapter include:

- *Internet Proxy Options* on page 13-1
- *SMTP Server Options* on page 13-2
- *Desktop/Server Options* on page 13-3
- *System Options* on page 13-7

Internet Proxy Options

If your network uses a proxy server to connect to the Internet, you must configure the Internet proxy settings in order to accomplish the following tasks:

- Download updates from the Trend Micro ActiveUpdate server
- View product license information
- Participate in the World Virus Tracking program

To set the Internet Proxy:

1. On the main menu, click **Preferences > Global Settings**.
2. Select the **Proxy** tab and the main frame changes to display proxy configuration options.

FIGURE 13-1. Global Settings

TREND MICRO Security Dashboard for SMB Log Off **TREND MICRO**

Live Status | Security Settings | Outbreak Defense | Scans | Updates | Reports | **Preferences** | Help

Preferences > Global Settings

Global settings apply to all computer(s) on the entire network.

Proxy | SMTP | Desktop/Server | System

☐ Use a proxy server for updates, online license renewal, and world virus tracking

Settings

Address: (examples: proxy.trend.com.tw or 123.123.123.123)

Port: 80

☐ Use SOCKS 4/5 proxy protocol

Proxy Password

User name:

Password:

Global Settings | Password | Tools | Product License | World Virus Tracking

3. Select the **Use a proxy server for updating components, product license notifications, and World Virus Tracking** check box.
4. Type the address of the proxy server and its port number.
 - If the proxy server uses version 4 or 5 of the SOCKS protocol to handle Transmission Control Protocol (TCP), select the **Use SOCKS 4/5 proxy protocol** check box.
5. If the proxy server requires a password, type your user name and password in the fields provided.
6. Click **Save**.

SMTP Server Options

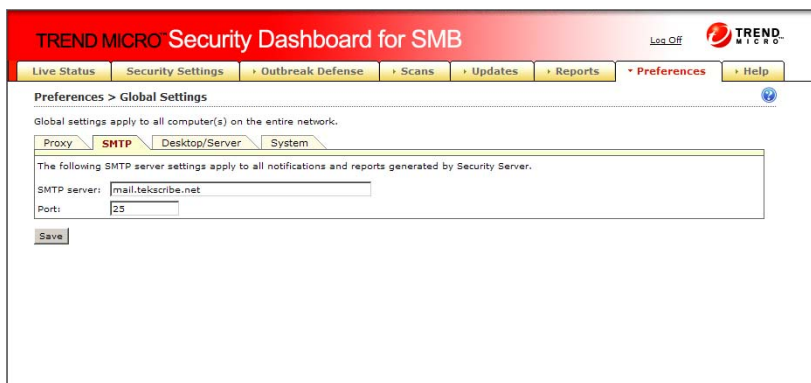
The SMTP Server settings apply to all notifications and reports generated by the Trend Micro Security Server.

To set the SMTP server:

1. On the main menu, click **Preferences > Global Settings**. The **Global Settings** screen appears.

2. Select the **SMTP** tab and the main frame changes to display SMTP configuration options.

FIGURE 13-2. Global Settings – SMTP Server Settings Screen



3. Type the IP address or name of the SMTP server.
4. Type the port number of the SMTP server.
5. Click **Save**.

Desktop/Server Options

The **Global Settings > Desktop/Server** screen contains the following configurable items.

- *General Scan Settings* on page 13-5
- *Virus Scan Settings* on page 13-5
- *Spyware/Grayware Scan Settings* on page 13-6
- *Alert Settings* on page 13-6
- *Approved List for Network Virus Scanning* on page 13-6
- *Watchdog Settings* on page 13-6
- *Agent Uninstallation* on page 13-7
- *Agent Unloading* on page 13-7

To set the Desktop/Server options:

1. On the main menu, click **Preferences > Global Settings**. The **Global Settings** screen appears.
2. Select the **Desktop/Server** tab and the main frame changes to display global desktop/server settings options.

FIGURE 13-3. Global Settings – Desktop/Server Settings Screen

TREND MICRO Security Dashboard for SMB Log Off

Live Status Security Settings Outbreak Defense Scans Updates Reports **Preferences** Help

Preferences > Global Settings

Global settings apply to all computer(s) on the entire network.

Proxy SMTP **Desktop/Server** System

General Scan Settings

- ☒ Exclude the Security Server database folder.
- ☒ Exclude Microsoft Exchange server folders when installed on Microsoft Exchange server.
- ☒ Exclude Microsoft Domain Controller folders (Not applicable to Manual and Scheduled spyware/grayware scans)

Virus Scan Settings

- ☒ Configure Scan Settings for large compressed files.
Do not scan if extracted size is over MB.
Scan the first files in the compressed file.
- ☒ Clean compressed files.
- ☒ Scan up to OLE layer(s).
- ☐ Add Manual Scan to the Windows shortcut menu on clients.

Spyware/Grayware Scan Settings

- ☒ Scan for cookies
- ☒ Count cookie into spyware log

Alert Settings

- ☒ Show the alert icon on the Windows taskbar if the virus pattern file is not updated after day(s).

Approved List for Network Virus Scanning

Add trusted computer(s) to the approved list to prevent them being identified as network viruses.

☐ Enable approved list for network virus scanning

IP address:

Watchdog Settings

- ☒ Enable the Client/Server Security Agent watchdog service:
Check client status every minute(s).
If the client cannot be started, retry times.
- ☒ Enable anti-hacking mode.

Agent Uninstallation

- ☐ Allow the client user to uninstall Client/Server Security Agent

3. Select the options you would like to enable.
4. Enter additional details as needed.
5. Click **Save**.

The following sections describe the options that you can configure on the **Desktop/Server** tab.

General Scan Settings

- **Exclude the Security Server database folder from real-time scan** – Select this check box to prevent Client Server Security from scanning its own database during Real-time Scans only

Note: By default, Client Server Security does not scan its own database. Trend Micro recommends preserving this selection to prevent any possible corruption of the database that may occur during scanning.

- **Exclude Microsoft Exchange server folders when installed on Microsoft Exchange server** – Select this check box to skip scanning of Microsoft Exchange folders when CSA is installed on the server
- **Exclude Microsoft Domain Controller folders** – Select this check box to skip scanning of Domain Controller folders when CSA is installed on the server

Virus Scan Settings

- **Configure scan settings for large compressed files** – Select this check box to specify which compressed files the Client/Server Security Agent will skip based on the size of each extracted file or number of files contained within the compressed file
- **Clean compressed files** – Select this check box if you want to clean compressed files
- **Scan up to { } OLE layer(s)** – Select this check box if you want your clients to scan Object Linking and Embedding (OLE) layers and then specify how many layers to scan. OLE allows users to create objects with one application and then link or embed them in a second application.
- **Add Manual Scan to the Windows shortcut menu on clients** – Select this check box if you want to create a link to a client's shortcut menu. Using the **Scan with Client/Server Security Agent** link on the shortcut menu allows users to scan files and folders by just right clicking a file or folder on the Windows desktop or in Windows Explorer.

Spyware/Grayware Scan Settings

- **Scan for cookies** – Select this check box to check cookies that have been downloaded to clients and servers from visited Web sites and automatically delete spyware cookies. Detected spyware cookies are added to the spyware counter on the Live Status page.

Note: By default, Client Server Security 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.

- **Count cookie into spyware log** – Select this check box to record each detected spyware cookie to the spyware log

Alert Settings

- **Show the alert icon on the Windows taskbar if the virus pattern file is not updated after {} days** – Select this check box if you want to display the alert icon on your clients when the virus or spyware pattern file is outdated and select a number from the list.

Approved List for Network Virus Scanning

- **Enable approved list for network virus scanning** – Select this if you want to enable the approved list for network scanning to keep trusted computer(s) from being identified as network viruses.
- **IP address** – Enter the IP address of the computer you would like to add to the approved list, and click **Add**.

Watchdog Settings

- **Enable the Client/Server Security Agent watchdog service** – Select this check box if you want to enable the CSA watchdog service.
- **Check client status every {} minutes** – Choose how often the watchdog service should check client status.
- **If the client cannot be started, retry {} times** – Choose how many times the watchdog service should attempt to restart the CSA.

- **Enable anti-hacking mode** – Select this check box to enable anti-hacking mode.

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

Agent Uninstallation

Allow the client user to uninstall Client/Server Security Agent – Choose this option if you want to allow client user to remove the CSA without supplying a password.

Require a password for the client user to uninstall Client/Server Security Agent – Choose this option if you want to require the client user to supply a password before uninstalling the CSA.

Agent Unloading

- **Allow the client user to unload Client/Server Security Agent** – Choose this option if you want to allow client user to unload the CSA without supplying a password.
- **Require a password for the client user to unload the Client/Server Security Agent** – Choose this option if you want to require the client user to supply a password before unloading the CSA.

System Options

The System section of the Global Settings screen contains the following configurable items.

- *Removing Inactive Desktops/Servers* on page 13-8
- *Verifying Client-Server Connectivity* on page 13-9
- *Maintaining the Quarantine Folder* on page 13-10

To set the System options:

1. On the main menu, click **Preferences > Global Settings**. The **Global Settings** screen appears.
2. Select the **System** tab and the main frame changes to display global system settings options.

FIGURE 13-4. Global Settings – System Settings Screen

TREND MICRO Security Dashboard for SMB Log Off **TREND MICRO**

Live Status Security Settings Outbreak Defense Scans Updates Reports **Preferences** Help

Preferences > Global Settings

Global settings apply to all computer(s) on the entire network.

Proxy SMTP Desktop/Server **System**

Remove Inactive Client/Server Security Agent

☒ Enable automatic removal of inactive Client/Server Security Agent
Automatically remove a Client/Server Security Agent if inactive for days

Connection Verification

☒ Enable scheduled verification

☐ Hourly:
☒ Daily: Start time: : (hh:mm)
☐ Weekly:

Quarantine Maintenance

Specify the capacity of the quarantine folder and the maximum file size that Client/Server Security Agent can quarantine. These settings may affect the Security Server performance during a virus outbreak.

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

Total files quarantined: 0

Total files size: 0 bytes

Quarantine folder capacity: MB

Maximum size for a single file: MB

3. Select the options you would like to enable.
4. Enter additional details as needed.
5. Click **Save**.

The following sections describe the options that you can configure on the **System Settings** screen.

Removing Inactive Desktops/Servers

When you use the Client/Server Security Agent uninstallation program to remove the Client/Server Security Agent program from a computer, the program automatically

notifies the server. When the server receives this notification, it removes the client icon from the Security Groups Tree to show that the client does not exist anymore.

However, if the client is removed using other methods, such as reformatting the computer hard drive or deleting the client files manually, Client Server Security will not be aware of the removal and it will display the client as inactive. If a user unloads or disables the client for an extended time, the server also displays the client as inactive.

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

To enable the automatic removal of inactive CSAs, configure the following options:

- **Enable automatic removal of inactive Client/Server Security Agent** – Select this option to enable the automatic removal of clients that have not made contact with the Security server for a specific number of days.
- **Automatically remove a Client/Server Security Agent if inactive for {} days** – Choose the number of days that a client is allowed to be inactive before it is removed from the Security Dashboard.

Verifying Client-Server Connectivity

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

You can verify client-server connection manually or by schedule from the Security Dashboard.

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

You can perform verification of client-server connection automatically and manually by configuring the following options:

- **Enable scheduled verification** – Select this check box to enable scheduled verification of client-security server communication.
- **Verify Now** – Click this if you want to instantly test for client-security server connectivity.

Maintaining the Quarantine Folder

Whenever a client detects an Internet threat in a file and the scan action for that type of threat is quarantine, the Client/Server Security Agent program encrypts the infected file, places it in the Client/Server Security Agent's suspect folder, and sends it to the Trend Micro Security Server quarantine folder. Client Server Security encrypts the infected file to prevent it from infecting other files.

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

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

The default location of Trend Micro Security Server quarantine folder is as follows:

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

Note: If the client is unable to send the encrypted file to the Trend Micro Security Server for any reason, such as network connection problems, the encrypted file remains in the client's suspect folder. The client attempts to resend the file when it reconnects to the Trend Micro Security Server.

For more information on configuring scan settings, or changing the location of the quarantine folder, see [Virus Scan Settings](#) on page 13-5.

From the **Global Settings** screen, you can configure the capacity of the quarantine folder and the maximum individual file size for every infected file that can be stored in it.

The following options are available to help you manage the quarantine folder:

- **Quarantine folder capacity** – Type an amount in MB for the capacity of the Quarantine folder.
- **Maximum size for a single file** – Type an amount for the size of single folder stored in the Quarantine folder.

- **Delete All Quarantined Files** – Click this to delete all files in the Quarantine folder instantly.

Using Administrative and Client Tools

This chapter explains how to use the Administrative and Client tools that come with Client Server Security.

The topics discussed in this chapter include:

- *Tool Types* on page 14-1
- *Summary of Tools* on page 14-2
- *Administrative Tools* on page 14-2
- *Client Tools* on page 14-7

Tool Types

Client Server Security includes a set of tools that can help you easily accomplish various tasks, including server configuration and client management.

These tools are classified into two categories:

- **Administrative tools** – Developed to help configure the Trend Micro Security Server and manage clients
- **Client tools** – Developed to help enhance the performance of the Client/Server Security Agent program

Summary of Tools

Refer to Table Note: for a complete list of tools included in this version of Client Server Security

Note: Some tools available in previous versions of Client Server Security are not available in this version. If you require these tools, contact technical support.

TABLE 14-1. Client Server Security Tools

Administrative Tools	Client Tools
Login Script Setup: automate the installation of the Client/Server Security Agent program	Client Packager (ClnPack.exe): create a self-extracting file containing the Client/Server Security Agent program and components
Vulnerability Scanner (TMVS.exe): search for unprotected computers on your network	Restore Encrypted Virus (VSEncode.exe): open infected files that Client Server Security encrypted
	Touch Tool (TmTouch.exe): change the time stamp on a hot fix to automatically redeploy it
	Client Mover Tool (IPXfer.exe): transfer Client/Server Security Agents from one Security Server to another. Source and destination servers must be running the same Client Server Security version and operating system language.

Note: You cannot run these tools from the Security Dashboard. For instructions on how to run the tools, see the relevant section below.

Administrative Tools

This section contains information about the following Client Server Security administrative tools:

Login Script Setup

With Login Script Setup, you can automate the installation of the Client/Server Security Agent to unprotected computers when they log on to the network. Login Script Setup adds a program called `autopcc.exe` to the server login script. The program `autopcc.exe` performs the following functions:

- Determines the operating system of the unprotected client computer and installs the appropriate version of the Client/Server Security Agent
- Updates the virus pattern file and program files

For instructions on installing clients, see the Client/Server Security Agent online help.

Vulnerability Scanner

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

Vulnerability Scanner can perform the following functions:

- Perform a DHCP scan to monitor the network for DHCP requests so that when computers first log on to the network, Vulnerability Scan can determine their status
- Ping computers on your network to check their status and retrieve their computer names, platform versions, and descriptions
- Determine the antivirus solutions installed on the network. It can detect Trend Micro products (including OfficeScan, ServerProtect for Windows NT and Linux, ScanMail for Microsoft Exchange, InterScan Messaging Security Suite, and PortalProtect) and third-party antivirus solutions (including Norton AntiVirus Corporate Edition v7.5 and v7.6, and McAfee VirusScan ePolicy Orchestrator).
- Display the server name and the version of the pattern file, scan engine and program for OfficeScan and ServerProtect for Windows NT
- Send scan results via email
- Run in silent mode (command prompt mode)
- Install the Client/Server Security Agent remotely on computers running Windows Vista/2000/XP (Professional only)/Server 2003

You can also automate Vulnerability Scanner by creating scheduled tasks. For information on how to automate Vulnerability Scanner, see the TMVS online help.

To run Vulnerability Scanner on a computer other than the server, copy the TMVS folder from the \PCCSRV\Admin\Utility folder of the server to the computer.

Note: You cannot install the Client/Server Security Agent with Vulnerability Scanner if the server component of Client Server Security is **present** on the same machine. Vulnerability Scanner does not install the Client/Server Security Agent on a machine already **running** the server component of Client Server Security.

To configure Vulnerability Scanner:

1. In the drive where you installed the server component of Client Server Security, open the following directories: **Client Server Security > PCCSRV > Admin > Utility > TMVS**. Double-click **TMVS . exe**. The Trend Micro Vulnerability Scanner console appears.
2. Click **Settings**. The **Settings** screen appears.
3. In the **Product Query** box, select the products that you want to check for on your network. Select the **Check for all Trend Micro products** to select all products. If you have Trend Micro InterScan and Norton AntiVirus Corporate Edition installed on your network, click **Settings** next to the product name to verify the port number that Vulnerability Scanner will check.
4. Under **Description Retrieval Settings**, click the retrieval method that you want to use. Normal retrieval is more accurate, but it takes longer to complete.

If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting the **Retrieve computer descriptions when available** check box.

5. To send the results to you or other administrators automatically, under **Alert Settings** select the **Email results to the system administrator** check box, and then, click **Configure** to specify your email settings.
 - a. In **To**, type the email address of the recipient.
 - b. In **From**, type your email address. This will let the recipient know who sent the message, if you are not only sending it to yourself.

- c. In **SMTP server**, type the address of your SMTP server. For example, you can type smtp.company.com. The SMTP server information is required.
 - d. In **Subject**, type a new subject for the message or accept the default subject. Click **OK** to save your settings.
6. To display an alert on unprotected computers, select the **Display alert on unprotected computers** check box. Then, click **Customize** to set the alert message. The **Alert Message** screen appears. You can type a new alert message or accept the default message. Click **OK**.
 7. To save the results as a comma-separated value (CSV) data file, select the **Automatically save the results to a CSV file** check box. By default, CSV data files are saved to the TMVS folder. If you want to change the default CSV folder, click **Browse**. The **Browse for folder** screen appears. Browse for a target folder on your computer or on the network and then click **OK**.
 8. You can enable Vulnerability Scanner to ping computers on the network to get their status. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout** text boxes.
 9. To remotely install the client component of Client Server Security and send a log to the server, type the server name and port number. If you want to remotely install the client component of Client Server Security automatically, select the **Auto-install Client Server Security Client for unprotected computer** check box.
 10. Click **Install Account** to configure the account. The **Account Information** screen appears.
 11. Type the user name and password and click **OK**.
 12. Click **OK** to save your settings. The **Trend Micro Vulnerability Scanner** console appears.
- To run a manual vulnerability scan on a range of IP addresses:**
1. Under **IP Range to Check**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers. Note that the Vulnerability Scanner only supports class B IP addresses.

2. Click **Start** to begin checking the computers on your network. The results are displayed in the **Results** table.

To run Vulnerability Scanner on computers requesting IP addresses from a DHCP server:

1. Click the **DHCP Scan** tab in the **Results** box. The **DHCP Start** button appears.
2. Click **DHCP Start**. Vulnerability scanner begins listening for DHCP requests and performing vulnerability checks on computers as they log on to the network.

To create scheduled tasks:

1. Under **Scheduled Tasks**, click **Add/Edit**. The **Scheduled Task** screen appears.
2. Under **Task Name**, type a name for the task you are creating.
3. Under **IP Address Range**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers.
4. Under **Task Schedule**, click a frequency for the task you are creating. You can set the task to run **Daily**, **Weekly**, or **Monthly**. If you click **Weekly**, you must select a day from the list. If you click **Monthly**, you must select a date from the list.
5. In the **Start time** lists, type or select the time when the task will run. Use the 24-hour clock format.
6. Under **Settings**, click **Use current settings** if you want to use your existing settings, or click **Modify settings**.

If you click **Modify settings**, click **Settings** to change the configuration. For information on how to configure your settings, refer to Step 3 to Step 12 of [To configure Vulnerability Scanner](#): on page 14-4

7. Click **OK** to save your settings. The task you have created appears under **Scheduled Tasks**.

Other Settings

To configure the following settings you need to modify `TMVS.ini`:

- **EchoNum** – Set the number of computers that Vulnerability Scanner will simultaneously ping.

- **ThreadNumManual** – Set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software.
- **ThreadNumSchedule** – Set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running scheduled tasks.

To modify these settings:

1. Open the TMVS folder and locate the `TMVS.ini` file.
2. Open `TMVS.ini` using Notepad or any text editor.
3. To set the number of computers that Vulnerability Scanner will simultaneously ping, change the value for `EchoNum`. Specify a value between 1 and 64.

For example, type `EchoNum=60` if you want Vulnerability Scanner to ping 60 computers at the same time.
4. To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software, change the value for `ThreadNumManual`. Specify a value between 8 and 64.

For example, type `ThreadNumManual=60` to simultaneously check 60 computers for antivirus software.
5. To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running scheduled tasks, change the value for `ThreadNumSchedule`. Specify a value between 8 and 64.

For example, type `ThreadNumSchedule=60` to simultaneously check 60 computers for antivirus software whenever Vulnerability Scanner runs a scheduled task.
6. Save `TMVS.ini`.

Client Tools

This section contains information about Client Server Security client tools.

Client Packager

Client Packager is a tool that can compress setup and update files into a self-extracting file to simplify delivery via email, CD-ROM, or similar media. It also includes an email function that can access your Microsoft Outlook address book and allow you to send the self-extracting file from within the tool's console.

To run Client Packager, double-click the file. Client Server Security clients that are installed using Client Packager report to the server where the setup package was created.

Restore Encrypted Virus

Whenever Client Server Security detects an infected file, it encrypts this file and stores it in the `Suspect` folder of the client, normally in `C:\Program Files\Trend Micro\Client Server Security Agent\SUSPECT`. The infected file is encrypted to prevent users from opening it and spreading the virus to other files on the computer.

However, there may be some situations when you have to open the file even if you know it is infected. For example, an important document has been infected and you need to retrieve the information from the document, you will need to decrypt the infected file to retrieve your information.

You can use Restore Encrypted Virus to decrypt infected files from which you want to open.

Note: To prevent Client Server Security from detecting the virus again when you use Restore Encrypted Virus, exclude the folder to which you decrypt the file from Real-time Scan.

WARNING! *Decrypting an infected file may spread the virus to other files.*

Restore Encrypted Virus requires the following files:

- Main file: `VSEncode.exe`
- Required DLL file: `Vsapi32.dll`

To decrypt files in the Suspect folder:

1. On the client where you want to decrypt an infected file, open Windows Explorer and go to the `\PCCSRV\Admin\Utility\VSEncrypt` folder of Client Server Security.
2. Copy the entire `VSEncrypt` folder to the client computer.

Note: Do not copy the `VSEncrypt` folder to the Client Server Security folder. The `Vsapi32.dll` file of Restore Encrypted Virus will conflict with the original `Vsapi32.dll`.

3. Open a command prompt and go to the location where you copied the `VSEncrypt` folder.
4. Run Restore Encrypted Virus using the following parameters:
 - `no parameter`: encrypt files in the Suspect folder
 - `-d`: decrypt files in the Suspect folder
 - `-debug`: create debug log and output in the root folder of the client
 - `/o`: overwrite encrypted or decrypted file if it already exists
 - `/f: {filename}`: encrypt or decrypt a single file
 - `/nr`: do not restore original file name

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

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

Restore Encrypted Virus provides the following logs:

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

To encrypt or decrypt files in other locations:

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

For example, if you want to encrypt or decrypt files in `C:\My Documents\Reports`, type `C:\My Documents\Reports\*.*` in the text file. Then save the text file with an INI or TXT extension, for example, you can save it as `ForEncryption.ini` on the C: drive.

2. At a command prompt, run Restore Encrypted Virus by typing `VSEncode.exe -d -i {location of the INI or TXT file}`, where {location of the INI or TXT file} is the path of the INI or TXT file you created (for example, `C:\ForEncryption.ini`).

Touch Tool

The Touch Tool synchronizes the time stamp of one file with the time stamp of another file or with the system time of the computer. If you unsuccessfully attempt to deploy a hot fix (an update or patch that Trend Micro releases) on the Trend Micro Security Server, use the Touch Tool to change the time stamp of the hot fix. This causes Client Server Security to interpret the hot fix file as new, which makes the server attempt to deploy the hot fix again automatically.

To run the Touch Tool:

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

`\PCCSRV\Admin\Utility\Touch`

2. Copy the `TMTouch.exe` file to the folder where the file you want to change is located. If synchronizing the file time stamp with the time stamp of another file, put both files in the same location with the Touch tool.

3. Open a command prompt and go to the location of the Touch Tool.
4. Type the following:

```
TmTouch.exe <destination_filename> <source_filename>
```

where:

<destination_filename> = the name of the file (the hot fix, for example) whose time stamp you want to change

<source_filename> = the name of the file whose time stamp you want to replicate

If you do not specify a source filename, the tool sets the destination file time stamp to the system time of the computer.

Note: You can use the wildcard character "*" in the destination file name field, but not the source file name field.

5. To verify the time stamp changed, type `dir` in the command prompt or right click the file in Windows explorer and select **Properties**.

Client Mover

If you have more than one Client Server Security server on the network, you can use Client Mover to transfer clients from one Client Server Security server to another. This is especially useful after adding a new Client Server Security server to the network when you want to transfer existing clients to the new server. The two Client Server Security servers must be of the same type and same language version.

Client Mover requires the `IPXfer.exe` file.

To run Client Mover:

1. On the Client Server Security server, go to the following directory:
`\PCCSRV\Admin\Utility\IPXfer`.
2. Copy the `IPXfer.exe` file to the client that you want to transfer.
3. On the client, open a command prompt and then go to the folder where you copied the file.
4. Run Client Mover using the following syntax:

```
IPXfer.exe -s <server_name> -p <server_listening_port> -m 1  
-c <client_listening_port>
```

where:

- <server_name> = the server name of the destination Client Server Security server (the server to which the client will transfer)
- <server_listening_port> = the listening (trusted) port of the destination Client Server Security server. To view the listening port on the Security Dashboard, click **Security Settings**. The listening port is shown next to the Security Server name.
- 1 = You must use the number "1" after "-m"
- <client_listening_port> = the port number of the client machine

To confirm the client now reports to the other server, do the following:

1. On the client, right click the CSA icon in the system tray.
2. Click **Client/Server Security Agent Console**.
3. Click **Help** on the menu, and then click **About**.
4. Verify that the Client Server Security server that the client reports to has been updated under **Communication information, Server name/port**.

Performing Additional Administrative Tasks

The topics discussed in this chapter include:

- *Changing the Security Dashboard Password* on page 15-2
- *Viewing Product License Details* on page 15-3
- *Participating in the World Virus Tracking Program* on page 15-3

Changing the Security Dashboard Password

To prevent unauthorized users from modifying your settings or removing the Client/Server Security Agent program from your computers, the Security Dashboard is password-protected. The Client Server Security master setup program requires you to specify a Security Dashboard password; however, you can modify your password from the Security Dashboard.

To change the Security Dashboard password:

1. On the main menu, click **Preferences > Password**. The **Administration Password** screen appears.

FIGURE 15-1. Preferences – Password Screen



The screenshot shows the 'Trend Micro Security Dashboard for SMB' interface. At the top, there is a red header bar with the product name and a 'Log Off' link. Below the header is a navigation menu with tabs: 'Live Status', 'Security Settings', 'Outbreak Defense', 'Scans', 'Updates', 'Reports', 'Preferences' (which is highlighted), and 'Help'. The main content area is titled 'Preferences > Password'. It contains a sub-header 'Set up the password for logging on to Trend Micro Security Dashboard for SMB.' followed by three text input fields labeled 'Old password:', 'New password:', and 'Confirm password:'. Below these fields is a note: 'Note: Passwords must be 1-24 any characters.' and a 'Save' button.

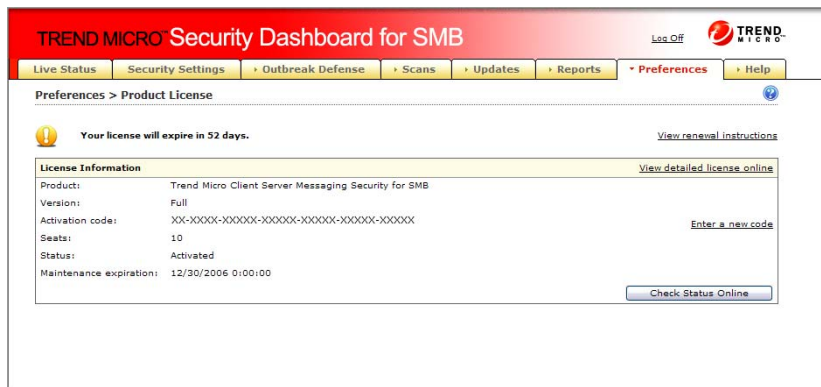
2. Type your current password in the **Old password** text box.
3. Type your new password (maximum 24 characters) in the **New password** text box, and then retype that password in the **Confirm password** text box.
4. Click **Save**.

Note: If you forget the Security Dashboard password, contact Trend Micro technical support for instructions on how to gain access to the Dashboard again. The only other alternative is to remove and reinstall Client Server Security.

Viewing Product License Details

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

FIGURE 15-2. Preferences – Product License Screen



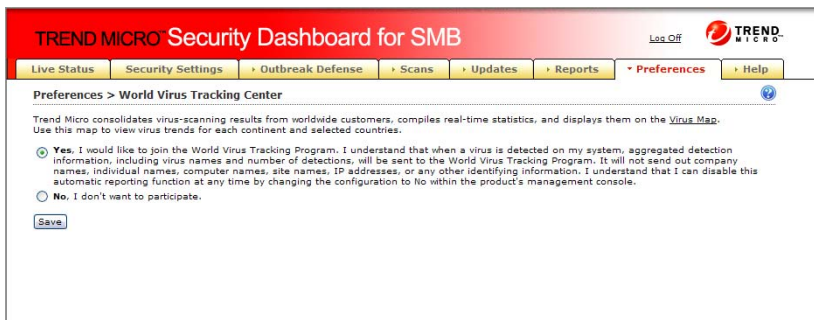
Participating in the World Virus Tracking Program

You can send virus scanning results from your Client/Server Security Agent installation to the World Virus Tracking Program to better track trends in virus outbreaks. Your participation in this program can benefit attempts to better understand the development and spread of virus infections.

When you install Client Server Security, the installer asks you whether you want to participate in the World Virus Tracking Program; however, you can change this setting at any time.

To save Virus Tracking Program participation settings:

1. On the main menu, click **Preferences > World Virus Tracking**. The **World Virus Tracking Program** screen appears.

FIGURE 15-3. Preferences – World Virus Tracking Program Screen

2. Read the disclaimer and click **Yes** to participate in the World Virus Tracking Program or click **No** to decline participation.
3. Click **Save**.

To view the current Trend Micro virus map, click Virus Map or enter the following address in your Web browser:

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

Understanding the Threats

The topics discussed in this chapter include:

- *What Do the Terms Mean?* on page 16-2
- *Viruses* on page 16-2
- *Trojans* on page 16-4
- *Bots* on page 16-4
- *Packers* on page 16-4
- *Worms* on page 16-4
- *About Mass-Mailing Attacks* on page 16-5
- *About Macro Viruses* on page 16-6
- *Guarding Against Malicious or Potentially Malicious Applications* on page 16-6

What Do the Terms Mean?

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

Some of these terms refer to real security risks and some refer to relatively harmless, but annoying or unsolicited incidents. Trojans, viruses, and worms are examples of terms used to describe real security risks. Joke programs and other grayware are terms used to describe incidents that might be harmful, but are sometimes simply annoying and unsolicited. The Messaging Security Agent can protect Exchange servers against all of the incidents described in this chapter.

Viruses

A computer virus is a segment of code that has the ability to replicate. Viruses usually replicate by infecting files. When a virus infects a file, it attaches a copy of itself to the file in such a way that when the former executes, the virus also runs. When this happens, the infected file also becomes capable of infecting other files. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate.

In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

Generally, there are three kinds of viruses:

- **File** – File viruses may come in different types— there are DOS viruses, Windows viruses, macro viruses, and script viruses. All of these share the same characteristics of viruses except that they infect different types of host files or programs.
- **Boot** – Boot viruses infect the partition table of hard disks and boot sector of hard disks and floppy disks.

- **Script** – Script viruses are viruses written in script programming languages, such as Visual Basic Script and JavaScript and are usually embedded in HTML documents.

VBScript (Visual Basic Script) and Jscript (JavaScript) viruses activate themselves using Microsoft's Windows Scripting Host. They then infect other files. Since Windows Scripting Host is available on Windows 98, Windows 2000 and other Windows operating systems, the viruses can be activated simply by double-clicking a *.vbs or *.js file from Windows Explorer.

What is so special about script viruses? Unlike programming binary viruses, which require assembly-type programming knowledge, virus authors programs script viruses as text. A script virus can achieve functionality without low-level programming and with code as compact as possible. It can also use predefined objects in Windows to make accessing many parts of the infected system easier (for example, for file infection, for mass-mailing). Furthermore, since the code is text, it is easy for others to read and imitate the coding paradigm. Because of this, many script viruses have several modified variants.

For example, shortly after the “I love you” virus appeared, antivirus vendors found modified copies of the original code, which spread themselves with different subject lines, or message bodies.

Whatever their type is, the basic mechanism remains the same. A virus contains code that explicitly copies itself. In the case of file viruses, this usually entails making modifications to gain control when a user accidentally executes the infected program. After the virus code has finished execution, in most cases, it passes back the control to the original host program to give the user an impression that nothing is wrong with the infected file.

Take note that there are also cross-platform viruses. These types of viruses can infect files belonging to different platforms (for example, Windows and Linux). However, such viruses are very rare and seldom achieve 100% functionality.

Network Viruses

A virus spreading over a network is not, strictly speaking, a network virus. Only some of the threats mentioned above, such as worms, qualify as network viruses. Specifically, network viruses use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of client

machines, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure. Because network viruses remain in memory, they are often undetectable by conventional disk-based file I/O scanning methods.

Personal Firewall works with a network virus pattern file to identify and block network viruses (see the on-line help for more information about configuring the Personal Firewall).

Trojans

A Trojan is a malicious program that masquerades as a harmless application. Unlike viruses, Trojans do not replicate but can be just as destructive. An application that claims to rid your computer of viruses when it actually introduces viruses onto your computer is an example of a Trojan. Traditional antivirus solutions can detect and remove viruses but not Trojans, especially those that are already running on the system.

Bots

Bots are compressed executable files that are designed with the intent to cause harm to computer systems and networks. Bots, once executed, can replicate, compress, and distribute copies of themselves.

Packers

Packers are compressed and/or encrypted Windows or Linux executable programs that are often Trojans. Compressing executables makes them more difficult for Antivirus products to detect.

Worms

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments. Unlike viruses, worms do not need to attach themselves to host programs. Worms often use email and applications, such as Microsoft™ Outlook™, to propagate. They may also drop copies of themselves into shared folders or utilize file-sharing systems,

such as Kazaa, under the assumption that users will likely download them, thus letting the worm propagate. In some cases, worms replicate themselves using chat applications such as ICQ, AIM, mIRC, or other Peer-to-Peer (P2P) programs.

About ActiveX

ActiveX is a technology from Microsoft that handles interaction between Web browsers, Microsoft applications, other third party applications, and the computer operating system. ActiveX makes use of ActiveX controls— software components installed on computers that add specialized functionality to Web pages, such as animation and interactive programs.

Creators of spyware and other grayware often mask their applications as legitimate ActiveX controls. When your users view Web sites that require ActiveX functionality, they may knowingly or unknowingly download the ActiveX controls to their computers and unwittingly install grayware applications.

Two related ways to help guard against spyware and other grayware that are masked as ActiveX controls are as follows:

- Setting client Web browser security to prompt the user before installing ActiveX applications
- Educating your users to look out for applications that could be grayware when they download any files, controls, or applications to their browsers

About Mass-Mailing Attacks

Email-aware viruses, like the infamous Melissa, Loveletter, AnnaKournikova and others, have the ability to spread via email by automating the infected computer's email client. Mass-mailing behavior describes a situation when an infection spreads rapidly between clients and servers in an Exchange environment. Mass-mailing attacks can be expensive to clean up and cause panic among users. Trend Micro designed the scan engine to detect behaviors that mass-mailing attacks usually demonstrate. The behaviors are recorded in the Virus Pattern file that is updated using the TrendLabs™ ActiveUpdate Servers.

About Macro Viruses

Macro viruses are application-specific. They infect macro utilities that accompany such applications as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications such as .doc, .xls, and .ppt. Macro viruses travel between data files in the application and can eventually infect hundreds of files if undeterred.

As these file types are often attached to email messages, macro viruses spread readily by means of the Internet in email attachments.

Guarding Against Malicious or Potentially Malicious Applications

You can take many steps to prevent the installation of spyware and other types of grayware onto your client computers. Trend Micro suggests making the following standard practices part of the anti-spyware/grayware initiative in your organization:

- Follow the recommended Client Server Security configuration steps in this chapter.
- Educate your client users to do the following:

Read the End User License Agreement (EULA) and included documentation of applications they download and install on their computers.

Click **No** to any message asking for authorization to download and install software unless the client users are certain both the creator of the software and the Web site they are viewing are trustworthy.

Disregard unsolicited commercial email (spam), especially if the spam asks users to click a button or hyperlink.

- Configure Web browser settings that ensure a strict level of security. Trend Micro recommends requiring Web browsers to prompt users before installing ActiveX controls. To increase the security level for Internet Explorer (IE), go to **Tools > Internet Options > Security** and move the slider to a higher level. If this setting causes problems with Web sites you want to visit, click **Sites...**, and add the sites you want to visit to the trusted sites list.
- If using Microsoft Outlook, configure the security settings so that Outlook does not automatically download HTML items, such as pictures sent in spam messages. Creators of spyware and grayware often use pictures.

- Disallow the use of peer-to-peer file-sharing services. Spyware and other grayware applications may be masked as other types of files your users may want to download, such as MP3 music files.
- Periodically examine the installed software on your client computers and look for applications that may be spyware or other grayware. If you find an application or file that Client Server Security cannot detect as grayware but you think is a type of grayware, send it to Trend Micro: <http://subwiz.trendmicro.com/SubWiz>. Trend Labs will analyze the files and applications you submit. If you prefer to communicate via email, send a message to the following address:

`virusresponse@trendmicro.com`

See *Contacting Technical Support* on page 17-12 for more information.

- Keep your Windows operating systems updated with the latest patches from Microsoft. See the Microsoft Web site for details.

FAQs, Troubleshooting and Technical Support

This chapter provides answers to commonly asked questions about installation and deployment, describes how to troubleshoot problems that may arise with Client Server Security, and provides information you will need to contact Trend Micro technical support.

The topics discussed in this chapter include:

- *Frequently Asked Questions (FAQs)* on page 17-2
- *Troubleshooting* on page 17-4
- *The Trend Micro Security Information Center* on page 17-10
- *Known Issues* on page 17-11
- *Contacting Technical Support* on page 17-12
- *The Trend Micro Knowledge Base* on page 17-12
- *Sending Suspicious Files to Trend Micro* on page 17-13
- *About TrendLabs* on page 17-13

Frequently Asked Questions (FAQs)

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

Registration

I have several questions on registering Client Server Security. Where can I find the answers?

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

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

Installation, Upgrade, and Compatibility

Which OfficeScan versions can upgrade to this version of Client Server Security?

This version of Client Server Security supports upgrade from: **CSM 3.0** and **CSM 3.5**.

Which client installation method is best for my network environment?

See the on-line help for a summary and brief comparison of the various client installation methods available.

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

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

Does Client Server Security support 64-bit platforms?

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

Can I upgrade to Client Server Security from Trend Micro™ ServerProtect?

No. Server Protect will have to be uninstalled then Client Server Security can be installed. See *Client Server Security Minimum Requirements* on page 3-4

Configuring Settings

I have several questions on configuring Client Server Security settings. Where can I find the answers?

You can download all Client Server Security documentation from the following site:

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

Documentation

What documentation is available with this version of Client Server Security?

This version of Client Server Security includes the following: *Administrator's Guide*, *Getting Started Guide*, readme file, and help files for the Security Dashboard, Master Installer, and Client/Server Security Agent.

Can I download the Client Server Security documentation?

Yes. You can download the Administrator's Guide, Getting Started Guide, and readme file from the following site:

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

I have questions/issues with the documentation. How can I provide feedback to Trend Micro?

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

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

Troubleshooting

This section helps you troubleshoot issues that may arise during installation, upgrade, migration, and deployment.

Restoring Program Settings after Rollback or Reinstallation

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

To restore program settings after rollback or reinstallation:

1. Back up the Trend Micro Security Server database to a location outside of the Client Server Security program directory.

WARNING! *Do not use any other type of backup tool or application.*

2. Manually back up the following files and folders from the folder: `Program Files\Trend Micro\Security Server\PCCSRV`
 - **ofcScan.ini** – Contains global client 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 Client Server Security quarantines infected files
 - **HTTDB folder** – Contains the Client Server Security database
3. Uninstall Client Server Security (see [Uninstalling the Trend Micro Security Server](#) on page 4-33).

4. Perform a fresh install (see *Performing a Custom Installation* on page 4-9).
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:

```
\Private\component.ini
```

- a. Get current virus pattern version from the new server.

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

```
ComponentName=Virus pattern
```

```
Version=xxxxxx 0 0
```

- b. Update the virus pattern version in the backup 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 Client Server Security database and the relevant files and folders on the target machine in the `PCSSRV` folder.
8. Restart the Trend Micro Security Server Master Service.

Some Client Server Security Components are not Installed

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

Unable to Access the Web Console

There are several potential causes of this problem.

Browser Cache

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

SSL Certificate

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

Virtual Directory Settings

There may be a problem with the virtual directory settings If you are running the Security Dashboard 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.

Do the following:

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

Also change the execute permissions of the client install virtual directory.

Incorrect Number of Clients on the Security Dashboard

You may see that the number of clients reflected on the Security Dashboard is incorrect.

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

Use the Verify Connection feature through the Security Dashboard to check for duplicate client records. For more information on the Verify Connection feature, refer to [Verifying Client-Server Connectivity](#) on page 13-9.

Unsuccessful Installation from Web Page or Remote Install

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

- Verify that client -server communication exists by using ping and telnet
- Verify that you have administrator privileges to the target computer where you want to install the client
- Check if TCP/IP on the client is enabled and properly configured
- Check if the target computer meets the minimum system requirements
- Check if any files have been locked
- If you have limited bandwidth, check if it causes connection timeout between the server and the client
- If you are using a proxy server for client-server communication, check if the proxy settings are configured correctly
- Open a Web browser on the client, type `http://{Server name}:{server port} /SMB/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with

the server. This also indicates that the problem may be in the server database; it may not have a record of the client computer.

Client Icon Does Not Appear on Security Dashboard after Installation

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

To resolve this, do the following:

- 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
- Open a Web browser on the client, type `http://{Trend Micro Security Server_Name}:{port number}/SMB/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client.

Issues During Migration from Third-party Antivirus Software

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

Client Migration

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

```
Uninstallation failed.
```

There are several possible causes for this error:

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

There are also several possible solutions for this error:

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

To manually remove third-party software:

- If the third-party software is registered to the Add/Remove Programs
 - a. Open the Control Panel.
 - b. Double-click **Add/Remove Programs**.
 - c. Select the third-party software from the list of installed programs.
 - d. Click **Remove**.
- If the third-party software is not registered to the Add/Remove Programs
 - a. Open the Windows registry.
 - b. Go to
HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Uninstall.
 - c. Locate the third-party software and run the uninstall string value.
 - d. If the third-party software's setup program is in MSI format:
 - Locate the product number
 - Verify the product number
 - Run the uninstall string

Note: Some product uninstallation keys are in the Product Key folder.

To modify the service for the third-party software:

1. Restart the computer in Safe mode.
2. Modify the service startup from automatic to manual.
3. Restart the system again.
4. Manually remove the third-party software.

To unload the service or process for the third-party software:

WARNING! *This procedure may cause undesirable effects to your computer if performed incorrectly. Trend Micro highly recommends backing up your system first.*

1. Unload the service for the third-party software.
2. Open the Windows registry, then locate and delete the product key.
3. Locate and delete the run or run service key.

Verify that the service registry key in

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services has been removed.

The Trend Micro Security Information Center

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

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

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of threats expected to trigger in the current week, and describes the 10 most prevalent threats around the globe for the current week
- View a Virus Map of the top 10 threats around the globe
- Consult the Virus Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes

- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
 - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other threats
 - The Trend Micro *Safe Computing Guide*
 - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
 - A glossary of virus and other security threat terminology
- Download comprehensive industry white papers
- Subscribe to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Web masters
- Read about TrendLabs™, Trend Micro's global antivirus research and support center

Known Issues

Known issues are features in Client Server Security software that may temporarily require a work around. Known issues are typically documented in the Readme document you received with your product. Readmes for Trend Micro products can also be found in the Trend Micro Update Center:

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

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

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

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

Contacting Technical Support

A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

You can contact Trend Micro via fax, phone, and email, or visit us at:

<http://www.trendmicro.com>

Speeding Up Your Support Call

When you contact the Knowledge Base, to speed up your problem resolution, ensure that you have the following details available:

- Microsoft Windows and Service Pack versions
- Network type
- Computer brand, model, and any additional hardware connected to your machine
- Amount of memory and free hard disk space on your machine
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

The Trend Micro Knowledge Base

Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in Knowledge Base are product FAQs, important tips, preventive antivirus advice, and regional contact information for support and sales.

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

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

If you cannot find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

Sending Suspicious Files to Trend Micro

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

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

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

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

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

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

`virusresponse@trendmicro.com`

In the United States, you can also call the following toll-free telephone number:
(877) TRENDAY, or 877-873-6328

About TrendLabs

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

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The

daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

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

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

System Checklists

Use the checklists in this appendix to record relevant system information as a reference.

Server Address Checklist

You must provide the following server address information during installation, as well as during the configuration of the Trend Micro Security Server to work with your network. Record them here for easy reference.

TABLE A-1. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Trend Micro Security Server information		
IP address	10.1.104.255	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Web server information		
IP address	10.1.104.225	

TABLE A-1. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Proxy server for component download		
IP address	10.1.174.225	
Fully Qualified Domain Name (FQDN)	proxy.company.com	
NetBIOS (host) name	proxyserver	
SMTP server information (Optional; for email notifications)		
IP address	10.1.123.225	
Fully Qualified Domain Name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	
SNMP Trap information (Optional; for SNMP Trap notifications)		
Community name	trendmicro	
IP address	10.1.194.225	

Ports Checklist

Client Server Security uses the following ports.

TABLE A-2. Port Checklist

PORT	SAMPLE	YOUR VALUE
SMTP	25	
Proxy	Administrator Defined	
Security Dashboard	4343	
Trend Micro Security Server	8080	
Client/Server Security Agent	21112	
Messaging Security Agent	16372	

Trend Micro Services

Trend Micro Outbreak Prevention Policy

The Trend Micro Outbreak Prevention Policy is a set of Trend Micro recommended default security configuration settings that are applied in response to an outbreak on the network.

The Outbreak Prevention Policy is downloaded from Trend Labs to the Trend Micro Security Server.

When the Trend Micro Security Server detects an outbreak, it determines the degree of the outbreak and immediately implements the appropriate security measures as stated in the Outbreak Prevention Policy.

Based on the Outbreak Prevention Policy, Automatic Threat Response takes the following preemptive steps to secure your network in the event of an outbreak:

- Blocks shared folders to help prevent viruses from infecting files in shared folders
- Blocks ports to help prevent viruses from using vulnerable ports to infect files on the network and clients
- Denies write access to files and folders to help prevent viruses from modifying files
- Displays an alert message on clients running the Client/Server Security Agent program when a possible outbreak detected

Trend Micro Damage Cleanup Services

Client Server Security uses Damage Cleanup Services (DCS) to protect your Windows computers against Trojans (or Trojan horse programs) and viruses.

The Damage Cleanup Services Solution

To address the threats posed by Trojans and viruses, DCS does the following:

- Detects and removes live Trojans and active malicious code applications
- Kills processes that Trojans and other malicious applications create
- Repairs system files that Trojans and malicious applications modify
- Deletes files and applications that Trojans and malicious applications drop

To accomplish these tasks, DCS makes use of these components:

- **Virus Cleanup Engine** – The engine Damage Cleanup Services uses to scan for and remove Trojans and Trojan processes
- **Damage cleanup template** – Used by the virus cleanup engine, this template helps identify Trojan files and processes so the engine can eliminate them

In Client Server Security, DCS runs on the client on these occasions:

- Client users perform a manual cleanup from the client main console
- You perform Cleanup Now on the client from the Trend Micro Security Dashboard for SMB
- Client users run Manual or Scheduled Scan.
- After hot fix or patch deployment (see for more information)
- When the Client Server Security service is restarted (the Client Server Security client Watchdog service must be selected to restart the client automatically if the client program unexpectedly terminates. Enable this feature on the **Global Client Settings** screen. See the *Administrator's Guide* and Client Server Security online help for details.)

Because DCS runs automatically, you do not need to configure it. Users are not even aware when it is executed because it runs in the background (when the client is running). However, Client Server Security may sometimes notify the user to restart their computer to complete the process of removing a Trojan or grayware application.

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:

- 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 security personnel can do further research to resolve the vulnerabilities and secure the network.
- View assessment histories and compare reports to better understand the vulnerabilities and the changing risk factors to network security.

Trend Micro IntelliScan

IntelliScan is a new method of identifying files to scan. For executable files (for example, .zip and .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 crucial applications on the client because it uses minimal system resources
- Shorter scanning period – Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

Trend Micro ActiveAction

Different types of viruses require different scan actions. Customizing scan actions for different types of viruses requires knowledge about viruses and can be a tedious task.

ActiveAction is a set of pre-configured scan actions for viruses and other types of Internet threats. The recommended action for viruses is Clean, and the alternative action is Quarantine. The recommended action for Trojans and joke programs is Quarantine.

If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:

- Time saving and easy to maintain – ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- Updateable scan actions – Virus writers constantly change the way viruses attack computers. To help ensure that clients are protected against the latest threats and the latest methods of virus attacks, new ActiveAction settings are updated in virus pattern files.

Trend Micro IntelliTrap

IntelliTrap detects malicious code such as bots in compressed files. Virus writers often attempt to circumvent virus 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 viruses in files compressed up to 20 layers deep using any of 16 popular compression types.

True File Type

When set to scan true file type, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named “family.gif,” it does not assume the file is a graphic file. Instead, the scan engine opens the file header and

examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that someone named to avoid detection.

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

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

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

About ActiveAction

Different types of viruses require different scan actions. Customizing scan actions for different types of viruses can be a tedious task. For this reason, Trend Micro created ActiveAction.

ActiveAction is a set of pre-configured scan actions for viruses and other types of threats. The recommended action for viruses is Clean, and the alternative action is Quarantine. The recommended action for Trojans and joke programs is Quarantine.

If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus, Trend Micro recommends using ActiveAction.

Using ActiveAction brings you the following benefits:

- **Effort-saving maintenance** – ActiveAction uses Trend Micro scan actions. You do not have to spend time customizing the scan actions.
- **Updateable scan actions** – Virus writers constantly change the way viruses attack computers.

To ensure that clients are protected against the latest threats and the latest methods of virus attacks, Trend Micro updates ActiveAction settings in every new pattern file.

Planning a Pilot Deployment

Before performing a full-scale deployment, Trend Micro recommends that you first conduct a pilot deployment in a controlled environment. A pilot deployment provides an opportunity to determine how features work and what level of support you will likely need after full deployment.

It also gives your installation team a chance to rehearse and refine the deployment process and test if your deployment plan meets your organization's antivirus needs.

Tip: Although this phase is optional, Trend Micro highly recommends conducting a pilot deployment before doing a full-scale deployment.

Choosing a Pilot Site

Choose a pilot site that matches your production environment. Try to simulate the type of network topology that would serve as an adequate representation of your production environment.

Creating a Rollback Plan

Trend Micro recommends creating a disaster recovery or rollback plan in case there are issues with the installation or upgrade process.

This process should take into account company information security policies, as well as technical specifics.

Deploying Your Pilot

Evaluate the different deployment methods (see *Overview of Installation and Deployment* on page 3-2) to see which ones are suitable for your particular environment.

Evaluating Your Pilot Deployment

Create a list of successes and failures encountered throughout the pilot process. Identify potential pitfalls and plan accordingly for a successful deployment. This pilot evaluation plan can be rolled into the overall production deployment plan.

Trend Micro Product Exclusion List

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

TABLE D-1. Trend Micro Product Exclusion List

Product Name	Installation Path Location
InterScan eManager 3.5x	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager\CurrentVersion ProgramDirectory=
ScanMail eManager (ScanMail for Exchange eManager) 3.11, 5.1, 5.11, 5.12	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange eManager\CurrentVersion ProgramDirectory=
SMLN eManager NT (ScanMail for Lotus Notes)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=
IWSS (InterScan Web Security Suite)	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=

TABLE D-1. Trend Micro Product Exclusion List

Product Name	Installation Path Location
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=
SMEX (ScanMail for Exchange)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir=

TABLE D-1. Trend Micro Product Exclusion List

Product Name	Installation Path Location
SMEX (ScanMail for Exchange) <i>Continued</i>	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\QuarantineManager QMDir= 1. Get exclusion.txt file path from HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion\HomeDir 2. Go to HomeDir path (e.g. C:\Program Files\Trend Micro\Messaging Security Agent\) 3. 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
IMS (IM Security)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security\CurrentVersion HomeDir= VSQuarantineDir= VSBakupDir= FBArchiveDir= FTCFArchiveDir=

Exclusion List for Exchange Servers

By default, when the Security Agent is installed on an Exchange server (2000 or later), it will not scan Exchange databases, 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\|M:\
```

For other MS recommended folders, please add them to scan exclusion list manually.

For more information, please see <http://support.microsoft.com/kb/245822/>

Client Side Information

Client Server Security differentiates three types of clients:

- Normal clients
- Roaming clients
- 32-bit and 64-bit clients

Normal clients are computers that have the Client/Server Security Agent installed and are stationary computers that maintain a continuous network connection with the Trend Micro Security Server.

Icons that appear in a client's system tray indicate the status of the normal client. See Table E-1 for a list of icons that appear on the normal client.

TABLE E-1. Icons that Appear on a Normal Client

Icon	Description	Real-time Scan
	Normal client	Enabled
	Pattern file is outdated	Enabled
	Scan Now, Manual Scan, or Scheduled Scan is running	Enabled
	Real-time Scan is disabled	Disabled

TABLE E-1. Icons that Appear on a Normal Client

Icon	Description	Real-time Scan
	Real-time Scan is disabled and the pattern file is outdated	Disabled
	Real-time Scan Service is not running (red icon)	Disabled
	Real-time Scan Service is not running and the pattern file is outdated (red icon)	Disabled
	Disconnected from the server	Enabled
	Disconnected from the server and the pattern file is outdated	Enabled
	Disconnected from the server and Real-time Scan is disabled	Disabled

Roaming Clients

Roaming clients are computers with the Client/Server Security Agent installation that do not always maintain a constant network connection with the Trend Micro Security Server (for example, notebook computers). These clients continue to provide antivirus protection, but have delays in sending their status to the server.

Assign roaming privileges to clients that are disconnected from the Trend Micro Security Server for an extended period.

Roaming clients get updated only on these occasions:

- When the client performs Update Now or performs a Scheduled Update.
- When client connects to the Trend Micro Security Server.

For more information on how to update clients, see the Trend Micro Security Server online help.

The status of a roaming client is indicated by icons that appear in its system tray. See Table E-2 for a list of icons that appear on roaming clients.

TABLE E-2. Icons that Appear on a Roaming Client

Icon	Description	Real-time Scan
	Roaming client (blue icon)	Enabled
	Real-time Scan is disabled	Disabled
	Pattern file is outdated	Enabled
	Real-time Scan is disabled and the pattern file is outdated	Disabled
	Real-time Scan Service is not running (red icon)	Disabled
	Real-time Scan Service is not running and the pattern file is outdated (red icon)	Disabled

32-bit and 64-bit Clients

The Client/Server Security Agent (CSA) supports Windows Vista/XP/Server 2003 computers that use x86 processor architecture, and x64 processor architecture. The table below shows a comparison between Client Server Security features for both 32-bit and 64-bit client computers:

TABLE E-3. 32-bit and 64-bit Client Features Comparison

Feature	32-bit clients	64-bit clients	Vista 32-bit clients	Vista 64-bit clients
Manual, Real-time, and Scheduled Scan for viruses and other malicious code				
Anti-spyware				
Personal firewall		N/A	N/A	N/A

TABLE E-3. 32-bit and 64-bit Client Features Comparison

Roaming mode				
Damage Cleanup Services		N/A		N/A
Mailscan		N/A	N/A	N/A
Outbreak Prevention Policy		N/A		N/A
Watch Dog		N/A		N/A
Manual Scan from the Windows shortcut menu		N/A		N/A
Anti-Rootkit		N/A		N/A
CSA installation using login scripts			N/A	N/A

Note: Client/Server Security Agent does not support the Itanium 2 Architecture (IA-64).

Spyware Types

The Trend Micro anti-spam engine can detect 21 types of spyware. The following table identifies these spyware types and provides a threat description for each type. These spyware types may appear in the **Spyware/Grayware Type** column on the Spyware/Grayware Log Details page.

Spyware Type	Threat Description
Trackware	Trackware is a generic term that describes software that collects a computers demographic and usage information and sends it to some remote server via the Internet, where it can be used by other people in a variety of different ways including marketing.
Adware	Adware is a type of software that displays advertisements on the computer screen while a computer is running. Typically, AdWare is built into software that performs some other primary task such as file sharing. The justification for AdWare is for the software developer to recover revenue via advertising instead of for instance charging for their software. Some Adware will collect the computers usage information (e.g. sites visited) and send it up to a remote server on the Internet where it is collected and processed for marketing purposes.

Spyware Type	Threat Description
Cookie	Cookies are small files that are created by your Web browser when you visit sites on the Internet. Typically, they are used as a convenience to remember frequently used information that is required for access to a particular Web site. They can also be used to track your visits to certain Web sites and can provide companies with information about frequency of visits and other profile information. The user is usually not aware that their surfing habits are being tracked. Trend Micro Anti-Spyware identifies cookies that are created by the most common advertising companies and allows you to clean them, which helps to ensure your privacy while surfing.
Dialer	A program that usually configures some sort of dial up configuration such as a dial-up-networking connection in Windows. The user either knowingly or unknowingly will end up using the dialer that calls a time-charged number that is usually billed to your credit card.
General	The threat type is not known, or is not yet classified.
KeyLogger/ Monitoring Software	A type of software can be either commercially sold or may be installed inadvertently via the Internet. This software can allow people to monitor you keystrokes, your computer screen, etc. and can even allow remote access.
Trojan	A type of software that is installed unknowingly, usually as a result of installing some other software, or viewing an email. Since it exists as a software program on the computer, the range of activity of a Trojan can be quite broad, from usage monitoring to remote control to customized collection and theft of information.
Suspect	This item is suspect, because Trend Micro Anti-Spyware detected some characteristics that match a known spyware.
Browser Hijacker	A type of software that changes settings in your Web browser. This often includes changing your browser's default home page.
Parasite	A type of software that piggybacks onto other software. This type of software may be installed without the user's knowledge or consent.
Browser Helper Object	A type of module that acts as a plugin to Internet Explorer browser. Some BHOs may monitor or manipulate your Web surfing.
Layered Service Provider	A type of module that acts as a plugin to your Network System. LSPs usually have low level access to your network and Internet data.
URL Shortcut	A shortcut to a URL that exists in your Internet Browser or your desktop.
Peer To Peer	Software that allows users to exchange shared files over the Internet.
Worm	Software that propagates by creating duplicates of itself on other computers.
Downloader	Software that manages the download of other software onto computers.

Spyware Type	Threat Description
Virus	Software that propagates itself by attaching to other valid programs, or by existing as a separate program.
EULAware	Software that contains a non-standard or questionable End User License Agreement. For example, a license agreement that states the software or license may be updated without first notifying the user and that the user agrees to any future changes made to the software and/or license agreement. EULAware may broadly permit the software to transmit any type of information to a server, including information unrelated to the function of the software application.
CoolWebSearch Variant	A particularly complex set of Browser Hijacker variants that require innovative detection and removal techniques.
Security Weakness	A medium/high risk security weakness that exists on your computer that could be used to compromise your systems security.

Glossary of Terms

The following is a list of terms in this document:

Term	Description
ActiveUpdate	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of components such as the virus pattern files, scan engines, and program files.
ActiveX malicious code	A type of virus that resides in Web pages that execute ActiveX controls.
administrator	The person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
Anti-spam	Refers to a filtering mechanism, designed to identify and prevent delivery of advertisements, pornography, and other "nuisance" mail.
attachment	A file attached to (sent with) an email message.
body (message body)	The content of an email message.

Term	Description
boot sector viruses	A sector is a designated portion of a disk (the physical device on which data is written and read). The boot sector contains the data used by your computer to load and initialize the computer's operating system. A boot sector virus infects the boot sector of a partition or a disk.
bots	Bots are compressed executable files that are designed with the intent to cause harm to computer systems and networks. Bots, once executed, can replicate, compress, and distribute copies of themselves.
clean	To remove virus code from a file or message.
Cleanup	Cleanup detects and removes Trojans and applications or processes installed by Trojans. It repairs files modified by Trojans.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture. Note that the online help uses the term "Client computer" in a special way to refer to computers that form a client-server relationship to the Client Server Messaging main program, the Security Server.
client computers	Client computers are all the desktops, laptops, and servers where CSAs are installed. Exchange servers protected by Messaging Security Agents are also considered to be Client computers. CSAs perform Antivirus scanning and Firewall configurations on Client desktops and servers. Messaging Security Agents perform Antivirus scanning, Anti-spam filtering, email Content Filtering, and Attachment Blocking on Exchange servers.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
COM and EXE file infectors	A type of virus that masquerades as an application by using a .exe or .com file extension.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
Content Filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
default	A value that pre-populates a field in the Security Dashboard. A default value represents a logical choice and is provided for convenience. Use default values as pre-set by Trend Micro or customize them as required.
Denial of Service Attack (DoS Attack)	An attack on a computer or network that causes to a loss of 'service', namely a network connection. Typically DoS attacks negatively affect network bandwidth or overload computer resources, such as memory.

Term	Description
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
Dynamic Host Control Protocol (DHCP)	A device, such as a computer or switch, must have an IP address to be connected to a network, but the address does not have to be static. A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network.
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. Lacing decryption codes, CSAs cannot scan encrypted files.
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.
Exceptions	Exceptions, in relation to the Firewall, are a list of ports and communication protocols that will not be blocked by the Firewall. Exceptions also describe the ports that you have set so that they are never blocked during Outbreak Defense protection measures.
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
File Transfer Protocol (FTP)	FTP is a standard protocol used for transporting files from a server to a client over the Internet. Refer to Network Working Group RFC 959 for more information.
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
firewall	Firewalls create a barrier between the Internet and your local network to protect the local network from hacker attacks and network viruses. Firewalls examine data packet to determine if they are infected with a network virus.

Term	Description
FQDN (fully qualified domain name)	A fully qualified domain name (FQDN) consists of a host and domain name, including top-level domain. For example, www.trendmicro.com is a fully qualified domain name: www is the host, trendmicro is the second-level domain, and .com is the top-level domain.
FTP (file transfer protocol)	FTP is a standard protocol used for transporting files from a server to a client over the Internet.
grayware	Files and programs, other than viruses, that can negatively affect the performance of the computers on your network. These include spyware, adware, dialers, joke programs, hacking tools, remote access tools, password cracking applications, and others. The OfficeScan scan engine scans for grayware as well as viruses.
hot fixes and patches	Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the OfficeScan server and/or client program.
Hyper Text Transfer Protocol (HTTP)	HTTP is a standard protocol used for transporting Web pages (including graphics and multimedia content) from a server to a client over the Internet.
HTTPS	Hypertext Transfer Protocol using Secure Socket Layer (SSL).
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition, and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet Protocol (IP)	"The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)
Intrusion Detection System (IDS)	Intrusion Detection Systems are commonly part of firewalls. An IDS can help identify patterns in network packets that may indicate an attack on the client.
local	The term "local" refers to a computer on which you are directly installing or running software, as opposed to a "remote" computer which is physically distant and/or connected to your computer through a network.
macro viruses	A type of virus encoded in an application macro and often included in a document.
malware	A malware is a program that performs unexpected or unauthorized actions. It is a general term used to refer to viruses, Trojans, and worms. Malware, depending on their type, may or may not include replicating and non replicating malicious code.
message body	The content of an email message.

Term	Description
Network virus	Viruses that use network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. They often do not alter system files or modify the boot sectors of hard disks. Instead, network viruses infect the memory of computers, forcing them to flood the network with traffic, which can cause slowdowns and even complete network failure.
Notifications	The Security Server can send your system administrator a notification whenever significant abnormal events occur on your Client computers. For example: You can set up a condition that whenever the CSA detects 40 viruses within one hour, the Security Server will send a notification to the system administrator.
Outbreak Defense	During Outbreak Defense, the Security Server enacts the instructions contained in the Outbreak Prevention Policy. The Trend Micro Outbreak Prevention Policy is a set of recommended default security configurations and settings designed by TrendLabs to give optimal protection to your computers and network during outbreak conditions. The Security Server downloads the Outbreak Prevention Policy from Trend Micro ActiveUpdate server every 30 minutes or whenever the Security Server starts up. Outbreak Defense enacts preemptive measures such as blocking shared folders, blocking ports, updating components, and running scans.
phishing incident	A Phish is an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click on a link that will redirect their browsers to a fraudulent Web site where the user is asked to update personal information such as passwords, social security numbers, and credit card numbers in an attempt to trick a recipient into providing private information that will be used for identity theft.
Phish sites	A Web site that lures users into providing personal details, such as credit card information. Links to phish sites are often sent in bogus email messages disguised as legitimate messages from well-known businesses.
Ping of Death	A Denial of Service attack where a hacker directs an oversized ICMP packet at a target computer. This can cause the computers buffer to overflow, which can freeze or reboot the machine.
Post Office Protocol 3 (POP3)	POP3 is a standard protocol for storing and transporting email messages from a server to a client email application.
port number	A port number, together with a network address - such as an IP number, allow computers to communicate across a network. Each application program has a unique port number associated with it. Blocking a port on a computer prevents an application associated with that port number from sending or receiving communications to other applications on other computers across a network. Blocking the ports on a computer is an effective way to prevent malicious software from attacking that computer.
privileges (desktop privileges)	From the Security Dashboard, administrators can set privileges for the CSAs. End users can then set the CSAs to scan their Client computers according to the privileges you allowed. Use desktop privileges to enforce a uniform antivirus policy throughout your organization.

Term	Description
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
remote	The term "remote" refers to a computer that is connected through a network to another computer, but physically distant from that computer.
rules (content filtering)	Content filtering rules are rules that you set up to filter the content of email messages. You define undesirable content and sources and set the Messaging Security Agent to detect and take action against such content violations.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
Secure Socket Layer (SSL)	SSL is a scheme proposed by Netscape Communications Corporation to use RSA public-key cryptography to encrypt and authenticate content transferred on higher-level protocols such as HTTP, NNTP, and FTP.
SSL certificate	A digital certificate that establishes secure HTTPS communication between the Policy Server and the ACS server.
security dashboard	The Security Dashboard is a centralized Web-based management console. You can use it to configure the settings of CSAs and Messaging Security Agents which are protecting all your remote desktops, servers and Exchange servers. The Trend Micro Security Dashboard for SMB is installed when you install the Trend Micro Security Server and uses Internet technologies such as ActiveX, CGI, HTML, and HTTP.
security server	When you first install Client Server Messaging Security, you install it on a Windows server that becomes the Security Server. The Security Server communicates with the CSAs and the Messaging Security Agents installed on Client computers. The Security Server also hosts the Security Dashboard, the centralized Web management console for the entire Client Server Messaging Security solution.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. Note that the online help uses the term "Security Server" in a special way to refer to the server that forms a client-server relationship with the computers on your network to which you have installed the CSAs.

Term	Description
Simple Mail Transport Protocol (SMTP)	SMTP is a standard protocol used to transport email messages from server to server, and client to server, over the internet.
SOCKS 4	A TCP protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model.
spam	Unsolicited email messages meant to promote a product or service.
Telnet	Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.
Test virus	An inert file that acts like a real virus and is detectable by virus-scanning software. Use test files, such as the EICAR test script, to verify that your antivirus installation is scanning properly.
Transmission Control Protocol (TCP)	A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.
TrendLabs	TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.
Trojan horses	Executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter.
updates	Updates describe a process of downloading the most up-to-date components such as pattern files and scan engines to your computer.
virus	A virus is a program that replicates. To do so, the virus needs to attach itself to other program files and execute whenever the host program executes.
vulnerability	A vulnerable computer has weaknesses in its operating system or applications. Many threats exploit these vulnerabilities to cause damage or gain unauthorized control. Therefore, vulnerabilities represent risks not only to each individual computer where they are located, but also to the other computers on your network.
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on.
worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email. A worm can also be called a network virus.

Index

A

- About the Virus Cleanup Engine 2-8
- Activation Codes 4-4
- administrator account
 - required for installation 4-6
- administrator privileges
 - required for installation 4-6

C

- capabilities
 - Client Server Security ??-1-7
- Client Server Security
 - capabilities 1-7
- Client/Server Security Agent
 - deployment considerations 3-6
 - listening port 4-6
 - overview 2-4
- Common Firewall Driver 2-9
- compatibility issues
 - third-party applications 4-3
- Configuring Personal Firewall – Simple Mode 7-12
- Configuring the Personal Firewall - Advanced Mode 7-13
- Current Status – Cleanup 8-6
- Current Status – Prevention 8-2
- Current Status – Protection 8-5

D

- Damage Cleanup engine 2-8
- Damage Cleanup services
 - how it works 2-8
- deployment
 - overview 3-2
 - Security Server, on dedicated server 3-9
- Disabling the Firewall 7-15
- domain name, Security Server
 - prepare before installing 4-5

E

- evaluation license
 - benefits 4-4
 - features 4-3

F

- firewall
 - deploy Security Server behind 3-6
- firewall, Windows XP
 - added to Exception list 3-6
- fully licensed
 - benefits 4-4
 - features 4-3

H

- hostname, Security Server
 - prepare before installing 4-5
- Hot Fixes 2-10

I

- incremental pattern file update
 - size of download 3-8
- installation
 - overview 3-2
- installation path, Client/Server Security Agent
 - prepare before installing 4-6
- Internet Connection Firewall (ICF)
 - removing 4-4
- IP address, Security Server
 - prepare before installing 4-5

L

- license
 - consequences of expiry 4-3

M

- macro viruses
 - explained 16-6

N

- network traffic
 - causes 3-7
 - deployment considerations 3-7
 - during pattern file updates 3-8
- Network Virus Pattern 2-9

O

- Outbreak Defense - Settings 8-8

P

- password, Security Dashboard

- prepare before installing 4-5
- Patches 2-10
- ports
 - Client/Server/Security Agent 4-6
 - modifying after installation 4-6
 - Security Server 4-6
- ports, warning
 - attacks on HTTP port (80 or 8080) 4-6
- Potential Threat 8-8
- prescan, Security Server
 - explanation 4-7
- proxy server
 - prepare details before installing 4-5

R

- Registration Key 4-4
- restart after installation 4-7

S

- Security Dashboard
 - overview 2-3
 - technologies used 2-3
- Security Server
 - deployment on a dedicated server 3-9
 - deployment with firewall 3-6
 - listening port 4-6
 - overview 2-4
- server
 - address, checklist A-1
- Service 2-10
- Simple Mail Transport Protocol (SMTP)
 - definition G-7
- SMTP server
 - prepare before installing 4-5
- SOCKS 4
 - definition G-7
- SQL server databases
 - excluding from scanning
 - performance
 - with SQL server data-bases 4-4
- standard alert
 - email 12-4

T

- Telnet
 - definition G-7
- test virus
 - definition G-7
- third party antivirus applications
 - removing
 - removing

third party antivirus applications 4-3

- Transmission Control Protocol (TCP)
 - definition G-7
- Trend Micro ActiveAction B-4
- Trend Micro IntelliScan B-3
- TrendLabs
 - definition G-7
 - updates Virus Cleanup Pattern 2-9
- Trojan horses
 - definition G-7

U

- Using Antivirus to Configure Real-time Scan 7-2
- Using Desktop Privileges 7-16
- Using Quarantine 7-19
- Using the Personal Firewall 7-8

V

- Virus Cleanup Pattern 2-9
- virus pattern file
 - size of download 3-8
- Vulnerability Pattern File 2-9

W

- Warning
 - back up before removing third-party antivirus software 17-10
 - change port number to prevent attacks on HTTP port 4-6
 - decrypting infected files 14-8
 - do not send installation package to wrong Client computer 5-11
 - never use real virus for testing 5-24
 - remove lockdown tool during installation 4-8
 - using back up tools 17-4
- Windows XP Firewall

added to Exception list 3-6

