



Client Server Security³

for Small and Medium Business



Getting Started 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 applicable user documentation, which are available from the Trend Micro Web site at:

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

Trend Micro, the Trend Micro t-ball logo, InterScan VirusWall, OfficeScan, Scanmail, TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 1998 - 2007 Trend Micro Incorporated. All rights reserved.

Document Part No. CSEM33117/70305

Release Date: March 2007

Protected by U.S. Patent No. 5,623,600; 5,889,943; 5,951,698; and 6,119,165.

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

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

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

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

Contents

Chapter 1: Introducing Client Server Security for Small and Medium Business

What's New in Version 3.6	1-2
What's Included in Client Server Security for SMB	1-2
The Security Server	1-2
The Security Dashboard	1-2
The Client/Server Security Agents	1-3
The Client Computers	1-3
The Client Server Security Components	1-4
How Client Server Security Protects Your Computers and Network	1-7
The Security Server	1-7
The Client/Server Security Agents	1-7
Outbreak Defense	1-8
Live Status and Notifications	1-8

Chapter 2: Before You Begin

About This Guide	2-2
Who Should Use the Getting Started Guide?	2-2
What Information Can I Find in the Getting Started Guide?	2-2
The Client Server Security Documentation	2-3
Registering Client Server Security	2-5
Activating Client Server Security	2-5
Changing Your License	2-5
Understanding Your License	2-6
License Versions	2-6
Renewing a Fully-licensed Version	2-6

Chapter 3: Installing Client Server Security

Installation Checklist	3-2
Minimum System Requirements	3-3
Overview of the Installation Process	3-4
Performing a Typical Installation	3-5

Part 1: Launch the Setup Program and Get Started with the Installation	3-6
Part 2 - Configuring the Security Server and Security Dashboard Settings	3-10
Upgrading from a Previous Version	3-15
Supported Upgrades	3-15
Unsupported Upgrades	3-15
Before You Upgrade	3-15
Upgrading from an Evaluation Version	3-16

Chapter 4: Working With the Security Dashboard

Updating the Components	4-2
About ActiveUpdate	4-2
Exploring the Security Dashboard	4-3
The Security Dashboard Features	4-4
Icons on the Security Dashboard	4-5
Using Live Status and Notifications	4-5
Setting Up Notifications	4-5
Using Live Status	4-6
Understanding Outbreak Defense	4-10
The Outbreak Defense Strategy	4-10
Current Status	4-12
Potential Threat	4-17
Setting Up Outbreak Defense	4-19
Working with Security Settings	4-21
Viewing the Security Settings Screen	4-21
Viewing the Client Server Security Security Groups Tree	4-22
Viewing the Security Settings Toolbar	4-24
Removing the Client/Server Security Agent from Desktops and Servers	4-26

Chapter 5: Configuring Security Tasks

Understanding the Threats	5-2
Malware	5-2
Viruses	5-2
Network Viruses	5-2
Trojans	5-3

Bots	5-3
Packers	5-3
Worms	5-3
Setting Up and Running Security Tasks	5-4
Setting Real-time Antivirus Options for Desktops and Servers	5-4
Setting Firewall Options for Desktops and Servers	5-5
Granting Desktop Privileges	5-5
Setting Up the Quarantine Folder for Desktops and Servers	5-6
Managing Reports	5-6
Setting Global Preferences	5-7
Chapter 6: Contacting Support	
Contacting Trend Micro	6-2
Contacting Technical Support	6-2
Speeding Up Your Support Call	6-2
Appendix A: Best Practices to Protect Your Computers and Network	
Appendix B: Glossary of Terms	

Introducing Client Server Security for Small and Medium Business

Designed to suit the needs of small-to-medium sized corporate IT networks, Trend Micro™ Client Server Security for Small and Medium Business provides network-wide desktop and server protection.

Network-wide desktop and server protection helps shield servers and computers on the network from virus threats. Computers on your network are kept up-to-date with the latest pattern files through centralized management and automatic updates of client installations.

Seamless integration with Microsoft™ Windows™ makes Client Server Security a powerful, multi-layered defense against viruses 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.

What's New in Version 3.6

Version 3.6 of Client Server Security for Small and Medium Business (SMB) brings a host of benefits to small and medium businesses that lack dedicated resources for antivirus management. This version of Client Server Security (CS) 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 *Client Server Security Administrator's Guide Appendix E* for a comparison of the CSA features on different platforms.

What's Included in Client Server Security for SMB

The Client Server Security for SMB is an integrated package that is designed to protect all the desktops, laptops, and servers on your network.

The Security Server

At the center of Client Server Security is the Security Server. The Security Server hosts the Security Dashboard, the centralized Web management console for the entire Client Server Security solution. The Security Server installs Security Agents to the other computers on your network. The computers where the Security Agents are installed form a client-server relationship with the Security Server. The Security Server provides the centralized location for viewing security status information, configuring the system security, downloading components, and storing logs on the database and the client computers.

In Figure 1-1, the Security Server is indicated by ①.

The Security Dashboard

The Security Dashboard is a centralized Web-based management console. You can use it to configure the settings of Client/Server 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.

The Client/Server Security Agents

The Client/Server Security Agents gather security information from the client computers that they protect and send the information back to the Security Server. For example, the Security Agents report virus or malware detections or the completion of component updates. The information displays in the Security Dashboard, and the Security Server uses it to generate logs and reports about the security status of your client computers and network.

The Client/Server Security Agents protect your file servers and desktop computers. In Figure 1-1, the Client/Server Security Agent is indicated by **A**

The Client Computers

The client computers are all the desktops, laptops, and servers where Client/Server Security Agents are installed. Antivirus and anti-spyware scanning, as well as, firewall configurations all take place on the client computers.

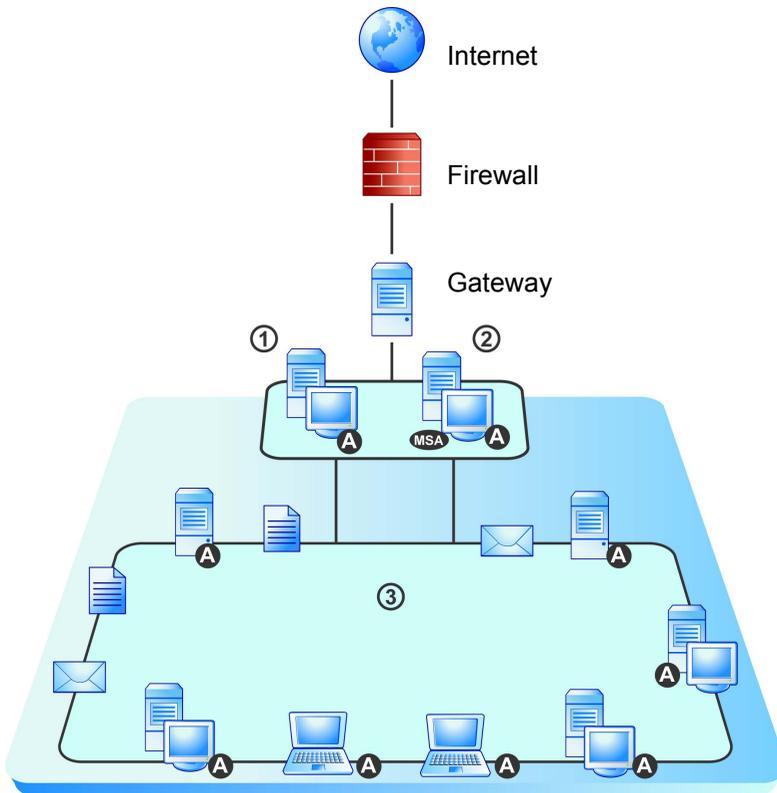


FIGURE 1-1. Client Server Security for SMB Protects Desktops and Servers

1. The Security Server
 2. Microsoft Exchange Server™ (not protected by Client Server Security)
 3. Local network
- A. Client/Server Security Agent

The Client Server Security Components

Client Server Security uses the following essential components:

Antivirus

- **Virus pattern**—a file that helps the Security Agents identify virus signatures, unique patterns of bits and bytes that signal the presence of a virus.
- **Scan engines**—the scan engine uses the virus pattern file to detect viruses and other security risks on files that your clients are opening and/or saving. The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique “signature” or string of tell-tale characters that distinguish it from any other code, the virus experts at 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.

Download the scan engine that matches your operating system.

- Scan engine for Windows 2000/Vista/XP/Server 2003
- Scan engine for Windows Vista/XP/Server 2003 on x64 architecture
- **Virus cleanup pattern**—used by the virus cleanup engine, this template helps identify Trojan files and processes so the engine can eliminate them.
- **Virus cleanup engine**—the engine that Cleanup Services uses to scan for and remove Trojans and Trojan processes.

Anti-spyware

- **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.

Network Virus

- **Common firewall pattern**—like the virus pattern file, this file helps Client Server Security identify network virus signatures.
- **Common firewall engine 32-bit**—the driver the Personal Firewall uses with the network virus pattern file to protect computers running Windows 2000/XP/Server 2003 from hacker attacks and network viruses.

Outbreak Defense

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

Other Supplementary Trend Micro Products

Client Server Security offers comprehensive protection for Windows desktops, laptops, and servers on a local network; however, it does not provide a solution for gateway devices and non-Windows operating systems, and mail servers.

To expand your protection, consider combining Client Server Security with Trend Micro™ InterScan VirusWall for Small and Medium Business, and/or Trend Micro™ ScanMail™ for Microsoft Exchange.

How Client Server Security Protects Your Computers and Network

Client Server Security is a multi-tier application that uses the following programs to protect your desktops, laptops, and servers:

The Security Server

The Security Server hosts the Security Dashboard (the Web-based management console that allows you to access the Security Server from any location connected to your network). The Security Server downloads critical component and policy updates and serves updated components to the Client/Server Security Agents. The Security Server also contains the database where it stores logs of detected viruses and malware being reported to it by the Security Agents.

The Client/Server Security Agents

The Client/Server Security Agents use antivirus scanning and Personal Firewall to protect your desktops, laptops, and servers from viruses, spyware, Trojans, worms, network viruses and other malware using the following technologies:

- **Antivirus scanning**
Antivirus scanning uses the Trend Micro scan engine and the virus pattern files to scan for viruses and other malware. By default, the Client/Server Security Agents use Real-time scanning, which you can customize. You can also set your own Scheduled scans or Manual scans.
- **Anti-spyware scanning**
Anti-spyware scanning uses separate scan engine and pattern files to scan for spyware on clients and servers. As with antivirus scanning, anti-spyware scanning provides three types of scans – Real-time, Scheduled, and Manual scans.

- **Personal Firewall**

Personal Firewall works with a network virus pattern file to identify and block network viruses. The Personal Firewall protects Windows 2000/XP/Server 2003 Client computers from hacker attacks and network viruses by creating a barrier between the client machine and the network.

- **POP3 Mail Scan**

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.

In addition, the Client Server Security solution uses the following features to automate and enhance the protection for your computers and network:

Outbreak Defense

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

Live Status and Notifications

Live Status gives you an at-a-glance security status for Outbreak Defense, Antivirus, Anti-spyware, and Network Viruses. Similarly, Client Server Security can send administrators notifications whenever significantly threatening events occur.

Before You Begin

This chapter instructs you on how to register and activate Client Server Security and where to find information about the product.

The topics discussed in this chapter include:

- *The Client Server Security Documentation* starting on page 2-3
- *About This Guide* starting on page 2-2
- *Understanding Your License* starting on page 2-6
- *Registering Client Server Security* starting on page 2-5
- *Activating Client Server Security* starting on page 2-5

About This Guide

Who Should Use the Getting Started Guide?

Network administrators for small-to-medium sized businesses who manage one or more Exchange servers and multiple desktops and servers.

What Information Can I Find in the Getting Started Guide?

Chapter 1: A brief introduction to the key features and benefits of Client Server Security

Chapter 2: Information about registering and activating Client Server Security and understanding your license

Chapter 3: Instructions on how to run a Typical installation which does not involve a Web server or configuring a proxy server

Chapter 4: A description of the Security Dashboard and how to use it to protect the computers on your network. The Security Dashboard is the centralized Web-management console for Client Server Security

Chapter 5: Instructions on how to configure and manage security tasks using Client Server Security

Chapter 6: How to find support

The Client Server Security Documentation

The Client Server Security documentation consists of the following:

- *Online Help*

Web-based documentation accessible from the Security Dashboard.

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

Who should use the Online Help? Network administrators for small and medium-sized businesses.

- *Getting Started Guide*

This *Getting Started Guide* was written to help small and medium-business network administrators to install the product and get started. It provides a description of the basic features and default settings of Client Server Security.

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

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

Who should read this Guide? Network administrators for small businesses who have relatively uncomplicated networks.

- *Administrator's Guide*

The *Administrator's Guide* provides a comprehensive guide to installing and deploying the product and understanding the features. It contains detailed information about upgrading and configuring Client Server Security.

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

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

Who should read this guide? Network administrators for medium-sized businesses who need to customize the installation or configurations.

- *Readme file*

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

Document Conventions

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

TABLE 1. Conventions Used in the Documentation

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and service or process names
<i>Italics</i>	References to other documentation
Monospace	Examples, sample command lines, program code, Web URLs, file names, folder names, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Registering Client Server Security

Your version of Client Server Security comes with a Registration Key. During installation, the Setup program prompts you to type your Activation Code. If you require an Activation Code, click the link from the Setup program to be redirected to the Trend Micro Web site where you can register online and receive an Activation Code.

You can register online any time at the following Trend Micro Web site:

<http://olr.trendmicro.com>

If you do not have either the Registration Key or Activation Code, contact your Trend Micro sales representative.

Activating Client Server Security

During installation, the Setup program prompts you to enter an Activation Code. If you leave the field empty, Client Server Security installs the Evaluation version. You can activate another version of your license any time from the Product License screen.

Changing Your License

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

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

1. Click **Preferences > Product License**.
2. Click **Enter a new code**.
3. Type your new Activation Code in the space provided.
4. Click **Activate**.

Understanding Your License

Your Client Server Security license entitles you to receive technical support and product updates. 60 days before the entitlement expires, the Security Dashboard will display a message in the Live Status screen, warning you to renew your license.

To renew your license, contact your Trend Micro reseller or visit Trend Micro online, at the following URL:

<https://olr.trendmicro.com/registration/>

License Versions

Trend Micro provides a fully licensed and an evaluation version of Client Server Security. Each version uses a different Activation Code.

Client Server Security for SMB

Designed to protect the desktops, laptops, and server computers on your local network. Includes Outbreak Defense, Firewall, and Antivirus scanning.

Client Server Security Evaluation Version

Test all the features of Client Server Security for SMB for a 30 trial. When the trial period ends, the Security Server no longer receives updated components.

Renewing a Fully-licensed Version

Contact your Trend Micro sales representative or corporate reseller to renew your license agreement. A Trend Micro representative will update your registration information on the Trend Micro Product Registration server.

The Security Server is set to poll the Product Registration server and receives the new expiry date directly from the Product Registration server. You are not required to manually enter a new Activation Code when renewing your license.

Consequences of an Expired License

When a full-version license expires, you can no longer download critical components such as the Virus Pattern file and Scan engine. However, when your Activation Code expires, all existing configurations and other settings remain in force. This provision maintains a level of protection in case you accidentally allow your license to expire.

Installing Client Server Security

This chapter instructs you on how to install or upgrade Client Server Security.

The topics discussed in this chapter include:

- *Installation Checklist* starting on page 3-2
- *Minimum System Requirements* starting on page 3-3
- *Overview of the Installation Process* starting on page 3-4
- *Performing a Typical Installation* starting on page 3-5
- *Upgrading from a Previous Version* starting on page 3-15
- *Upgrading from an Evaluation Version* starting on page 3-16

Installation Checklist

Trend Micro recommends verifying your system requirements and preparing the following information before you begin your installation.

During a Typical installation, the Setup program will prompt you to supply the following:

Registration Key and Activation Code

Register online and receive an Activation Code.

See *Exploring the Security Dashboard* on page 4-3.

Tip: If you do not type an Activation Code during the installation, you can complete the installation and run an Evaluation version of Client Server Security. When you are ready to use the fully licensed version, obtain a new Activation Code and type it in the Product License screen.

Security Server details

The domain/hostname or the IP address of the Security Server and the target directory where the Security Server files will be installed.

SMTP server

If using an SMTP server to send notifications, you require the name of the SMTP server, the port number, and the email address of notification recipients.

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 who tries to open the console.

Uninstall and Unload password

You will need this password to uninstall or unload the Client/Server Security Agent. Uninstalling removes the Client/Server Security Agent program from the Client computer. Unloading removes the Client/Server Security Agent from the menu taskbar.

Accounts and Privileges

You must log on with an administrator account with domain administrator privileges. If you do not log on with domain administrator privileges, you must manually create an administrative group before proceeding with the installation.

Minimum System Requirements

To install Client Server Security, the following are required:

TABLE 3-1. Installation Methods

Client Server Security Component	Minimum System Requirement				Other Requirements
	CPU	RAM	Disk Space	Operating System	
Security Server	733MHz	512MB	1GB	Win 2000 SP2 Win XP SP1 (R2) SBS 2000 SBS 2003 (R2)	Web Server: IIS5.0 IIS6.0 Apache 2.0.54 Web Console: IE5.5 (Hi-color display adaptor with 1024x768 resolution)
Client/Server Security Agent	300MHz	128MB	200MB	Windows Vista Win 2000 SP2 Win XP Win 2003 (R2) SBS 2000 SBS 2003 (R2)	Monitor: 800x600 resolution

Notes

- Gigabit Network Interface Card (NIC) supported
- Tablet PC supported
 - The Client/Server Security Agent supports all 64-bit CPU which includes:
 - AMD Athlon 64, AMD Opteron, Intel Xeon with Intel EM64T support, Intel Pentium 4 with Intel EM64T support
- Report format(.pdf) requires Acrobat Reader version 4.x

Overview of the Installation Process

Client Server Security offers three installation methods. This guide describes the Typical installation method. The other installation methods are Custom and Silent installation. For instructions on how to perform a Custom or Silent installation or for a more in-depth discussion about the installation process, refer to the *Administrator's Guide*.

TABLE 3-2. Installation Methods

Method	When to Use This Method
<p>Typical</p> <p>A Typical installation uses Trend Micro recommended defaults for some installation options.</p>	<ul style="list-style-type: none"> • You have a small network, configured in a simple manner
<p>Custom</p> <p>A Custom installation allows you to configure all options.</p>	<ul style="list-style-type: none"> • Your network contains many desktops and servers • You need to customize your proxy server or Web server settings
<p>Silent</p> <p>A Silent installation records a file that you can use to perform identical installations on other computers or networks.</p>	<ul style="list-style-type: none"> • You need to do multiple installations on similar networks. For example, you are a service provider who wants to use Client Server Security to protect your customer's networks.

An installation generally follows the following consecutive stages:

1. Launching the Setup program and registering Client Server Security.
2. Setting up the computer on which you will install the Security Server (the server-side program) and the Security Dashboard (the centralized Web console you use to manage the Security Server and client computers). This computer will become the Security Server.

Note: The computer on which you install Client Server Security is referred to as the "local" server, as opposed to a "remote" server which is located in a physically distant place connected to the same network as the local computer.

3. Setting up the local server on which you will install the Client/Server Security Agent.

Following the installation, Client Server Security deploys Client/Server Security Agents to all the desktops, laptops, and servers connected to your local network. If you are upgrading, Client Server Security preserves your previous configurations in the new version. All the Client computers protected by Client Server Security can be viewed in the Security Settings screen.

Performing a Typical Installation

Trend Micro designed the Client Server Security Setup default values to provide optimal protection for a typical small and medium-sized business. We recommend that you accept these values. However; if you want to customize these settings, consult the *Administrator's Guide* for a more in-depth discussion of installation options and consider running a Custom installation.

Part 1: Launch the Setup Program and Get Started with the Installation

To launch the Setup installation program:

- Install from the Trend Micro CD:
 - a. Insert the CD
 - b. Select your installation option (Client Server Security for SMB)
 - c. Click **Install**. The **Client Server Security Welcome** screen appears.
- Install by downloading the installation files:
 - a. Open the folder that contains the setup files.
 - b. Double-click **Setup** (SETUP.EXE). The **Client Server Security Welcome** screen appears.

To get started using Setup:

1. Click **Next**. The **Software License Agreement** screen appears.
2. Select **I accept the terms in the license agreement**.
3. Click **Next**. The **Product Activation** screen appears.

FIGURE 3-1. Product Activation Screen

4. If your product is not yet registered, click **Register Online**. When you click **Register Online** a browser window opens and is directed to the Trend Micro online registration page. The registration page requires that you type your Registration Key to obtain an Activation Code.
5. Type the Activation Code in the **Activation Code** field.
6. Click **Next**. The **Computer Prescan** screen appears.
7. Select **Prescan my computer for threats** to prescan the local computer to which you are installing Client Server Security.
The prescan includes a virus scan and Cleanup scan to help ensure the target computer does not contain viruses, Trojans, or other potentially malicious code. For more information, refer to the *Administrator's Guide*.
8. Click **Next**. The **Setup Type** screen appears.

FIGURE 3-2. Setup Type Screen

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

FIGURE 3-3. Installation Setup Overview Screen

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 3-4. Security Server Installation Stage Screen



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

FIGURE 3-5. Security Server Identification screen

3. Choose from one of the following Security Server identification options:
 - **Server information:** Trend Micro recommends using **Domain name**:
 - **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's IP address is correct. Selecting **IP Address** is not recommended if the computer on which the Security Server will be installed is subject to change (such as when the Security Server will obtain an IP address from a DHCP server).
 - **Target directory:** accept the default directory path provided or type a new directory path to which the Trend Micro Security Server files will be installed.

4. Click **Next**. The **SMTP Server and Notification Recipient(s)** screen appears.

FIGURE 3-6. SMTP Server and Notification Recipient(s) Screen

Trend Micro Client Server Security for SMB

SMTP Server and Notification Recipient(s)

Setup the SMTP server for sending all notifications and reports generated by Trend Micro Security Server.

SMTP server: 192.168.1.2

Port: 25

Recipient(s): Admin@NotRealSite.com

(Use semicolon ";" to separate multiple addresses.
For example: user1@domain.com;user2@domain.com)

InstallShield

< Back Next > Cancel

5. The **SMTP Server and Notification Recipient(s)** screen requires the following information:
 - **SMTP Server** – type the name of the SMTP Server. For example, type `smtp.company.com`
 - **Port** - by default SMTP uses port 25 to communicate
 - **Recipient(s)** - type the email addresses of all the people who will receive notifications and reports from the Security Server

FIGURE 3-7. Administrator Account Password Screen

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

Type the passwords in the Password fields provided and then confirm the passwords by typing them a second time in the Confirm Password field.

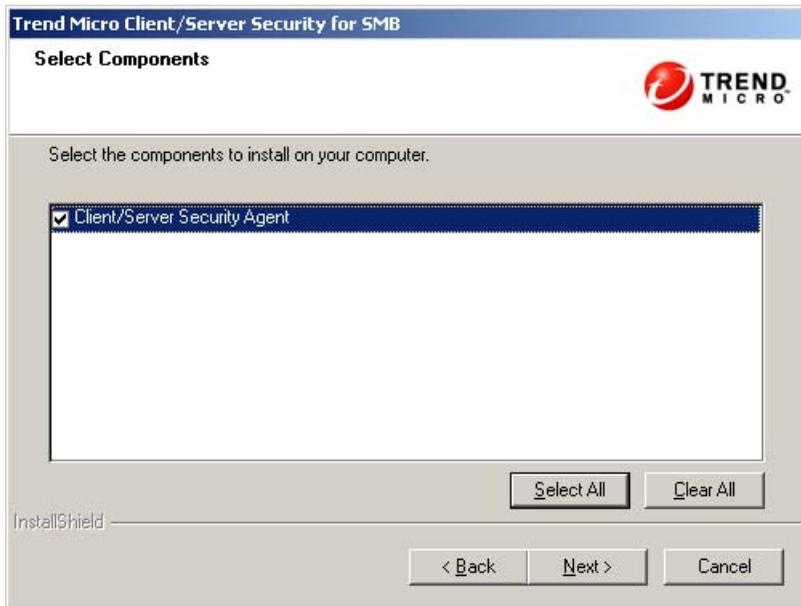
- **Security Dashboard** – following installation, use this password to access the Security Dashboard
- **Client/Server Security Agents** – following installation, use this password to unload or uninstall the Client/Server Security Agent from the Security Dashboard

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

7. Click **Next**. The **World Virus Tracking Program** screen appears. Refer to the *Administrator's Guide* for more information about the **World Virus Tracking Program**.

8. Click **Next**. The **Component Selection** screen appears.

FIGURE 3-8. Component Selection Screen



9. Select the components to install.
 - **Client/Server Security Agent** – install the Client/Server Security Agent on the same computer to which you are installing the Security Server
This is necessary for running security tasks on the Security Server computers.
10. Click **Next**. The **Review Settings** screen appears.
11. Click **Next**. The **Setup Status** screen showing you the progress of the installation. When the installation is complete, the Install Wizard Complete screen appears.
12. Click **Finish** to exit the installation Wizard.

Upgrading from a Previous Version

Upgrading refers to running Setup to install a newer version of Client Server Security on the existing server. The upgrade procedure is very similar to the normal installation process except that when specifying the server on which to install Security Server, you select your existing Security Server. The Client/Server Security Agents will upgrade automatically.

See *Overview of the Installation Process* on page 3-4.

Supported Upgrades

Client Server Security supports upgrade from any of the following versions:

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

Unsupported Upgrades

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

- Upgrade from Client/Server Suite 2.0
- Upgrade from OfficeScan Enterprise Edition
- Upgrade from one language to another

Before You Upgrade

Trend Micro recommends deleting all log files from the older Trend Micro Security server before upgrading.

You can preserve your client settings when you upgrade to the newest version of Client Server Security.

To ensure that you can easily restore your existing settings if the upgrade is unsuccessful, Trend Micro highly recommends backing up the older Security server database.

To back up the Security server database:

1. In Windows Explorer, go to the Security Server folder.
2. Go to the \PCCSRV\HTTPDB folder and copy the contents to another location (for example, to different directory on the same server, to another computer, or to a removable drive).

See also: For details about the effect of upgrading on your current settings and folders, refer to the *Administrator's Guide*.

Upgrading from an Evaluation Version

When your evaluation version is about to expire, a message displays on the **Live Status** screen. You can upgrade from an evaluation version to the fully-licensed version using the Security Dashboard. Your configuration settings will be saved. When you purchase a license to the fully-licensed version, you will be given a Registration Key or an Activation Code.

To upgrade from an evaluation 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, type it 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.

Working With the Security Dashboard

This chapter tells you how to get up and running with Client Server Security. It includes topics such as:

The topics discussed in this chapter include:

- *Updating the Components* starting on page 4-2
- *Exploring the Security Dashboard* starting on page 4-3
- *Using Live Status and Notifications* starting on page 4-5
- *Understanding Outbreak Defense* starting on page 4-10
- *Working with Security Settings* starting on page 4-21

Updating the Components

Both the Security Server and the Client computers require up-to-date components. Client Server Security makes this easy for you by having the Client computers automatically receive updated components from the Security Server.

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 components and the Outbreak Defense policy
- By default, Scheduled Updates run every hour to update the Security Server
- By default, the Client/Server Security Agent runs a Scheduled update every eight hours

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

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.

See also: For more information about customizing your component updates, refer to the *Administrator's Guide*.

About 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 virus pattern files, scan engines, and program files via the Internet. ActiveUpdate does not interrupt network services, or require you to reboot your computers.

Incremental updates of the virus pattern file

ActiveUpdate supports incremental updates of pattern files. Rather than download the entire pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software.

Using ActiveUpdate with Client Server Security

Click Trend Micro's ActiveUpdate Server from the **Updates > Update Source** screen to set the Security Server to use the ActiveUpdate server as a source for manual and scheduled component updates. When it is time for a component update, the Security Server polls the ActiveUpdate server directly. If a new component is available for download, the Security Server downloads the component from the ActiveUpdate server.

Exploring the Security Dashboard

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

To open the Security Dashboard:

1. Select one of the following options to open the Security Dashboard:
 - From the Windows Start menu, click:
`Trend Micro Client Server Security > Security Dashboard`
 - You can also open the Security Dashboard from any computer on the network. Open a Web browser and type the following in the address bar:
`http://{Security_Server_Name}:{port number}/SMB`
 - If using SSL, type the following in the address bar:
`https://{Security_Server_Name}:{port number}/SMB`
2. The browser displays the Trend Micro Security Dashboard for SMB login screen.

FIGURE 4-1. Login screen of the Security Dashboard

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

See *Using Live Status* on page 4-6.

The Security Dashboard Features

The following is a description of the major features of the Security Dashboard.

TABLE 4-1. Security Dashboard Main Features

Feature	Description
Main menu items	Along the top of the Security Dashboard are the main menu items. These menu items remain available regardless of the options you select.
Configurations area	Below the main menu items is the configuration area. Use this area to select options according to the menu item you selected.
Menu sidebar	When you choose a computer or group from the Security Settings screen and click Configure , a menu sidebar displays. Use the sidebar to configure security settings and scans.
Security Settings toolbar	When you open the Security Settings screen you can see a toolbar containing a number of icons. When you click on a computer or group from the Security Settings screen and click an icon on the toolbar, the Security Server performs the associated task.

Icons on the Security Dashboard

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

TABLE 4-2. Security Dashboard Icons

Icons on the Security Dashboard	
	Click the Help icon to open the online help.
	Click the Refresh icon to refresh the view of current screen.
	Click the Hidden text icon to display hidden text.
	Click the Quick Tour icon to view a tutorial about current screen features.
	Click the Information icon to display information pertaining to a specific item.

Using Live Status and Notifications

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

Setting Up Notifications

Use **Preferences > Notifications** to set up event notifications or customize parameters for the events.

Trend Micro recommended settings for Notifications

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

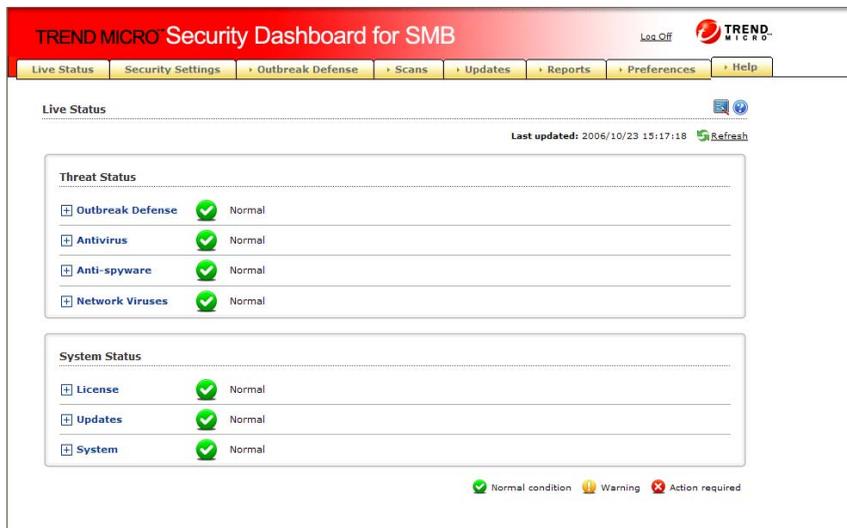
Clear the check boxes to cancel the notification. Click on a notification to display the notification content detail and customize those details, if necessary.

The following settings are the default values used by Client Server Security.

- **Antivirus**
Viruses detected on desktops/servers exceeds: 5 incidents within 1 hour.
- **Anti-spyware**
Spyware/Grayware detected on desktops/servers exceeds: 15 incidents within 1 hour.
- **Network Virus**
Network viruses detected exceeds: 10 incidents within 1 hour.
- **System Events**
The available free disk space is decreasing to less than: 1%.

Using Live Status

The Live Status screen is the first screen that displays when opening the Trend Micro Security Dashboard for SMB. All the information you need to know conveniently displayed on one screen.

FIGURE 4-2. Live Status Screen

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

The information displayed in Live Status is generated by the Security Server and based on data collected from the Client computers.

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

Threat Status

At-a-glance, view a status update about the threats to computers on your network. Threat Status reports security risks on your network based on Trend Micro recommended policies. The icons warn you if action is necessary to secure the computers on your network.

Outbreak Defense

The Security Server determines whether you have an outbreak problem based on policies that it downloads from Trend Micro. When there is a problem, the Security Server displays a Red or Yellow Alert icon and triggers Outbreak Defense. During Outbreak Defense, the Security Server might take protective actions such as blocking ports, downloading components, and running scans. You can view these actions by clicking **View** from the **Threat Information** panel in **Outbreak Defense > Current Status**.

During an outbreak alert, clicking the underlined link from the **Vulnerable Computers** or **Computers to Cleanup** opens the Current Threat screen to show you how the Security Server is protecting your computers and network. Under normal conditions, clicking these links opens the Potential Threats screen where you can view at risk computers and initiate scanning to check for vulnerabilities and cleanup damaged computers.

See *Understanding Outbreak Defense* on page 4-10.

About Red and Yellow Alerts

Trend Micro issues a red alert when it receives several reports of virus and other malware incidents in a short amount of time. The reports usually describe a virus or malware threat that is actively circulating on the Internet and spreading to mail servers and computers on local networks. Red alerts trigger the Trend Micro 45-minute Red Alert solution process. This process includes deploying an Official Pattern Release (OPR) and notifying designated computer security professionals, repressing all other notifications to conserve bandwidth, and posting fix tools and information regarding vulnerabilities to Trend Micro download pages.

Trend Micro issues a yellow alert when it receives several reports of virus and other malware incidents in a short amount of time. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download.

Antivirus

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

Anti-spyware

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

Network Viruses

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

By default, the information is refreshed every hour.

License

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

Updates

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

- To deploy updated components to Client computers, click **Deploy Now**
- To manually update the Security Server components, click **Update Now**

System

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

Understanding Outbreak Defense

Outbreak Defense is a key component of Client Server Security solution. Trend Micro designed Outbreak Defense to protect small and medium-sized businesses during times of virus and malware outbreaks.

The Outbreak Defense Strategy

The Outbreak Defense Strategy is based on the idea of an outbreak life cycle. The life of an outbreak is divided into three stages. Trend Micro counters each stage of the cycle with a defense strategy. The defense strategy is the Outbreak Defense

TABLE 4-3. Outbreak Defense Response to the Outbreak Life Cycle Stages

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

Outbreak Defense Actions

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

- 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 Client computers

Note: Outbreak Defense never blocks the port used by the Security Server to communicate with the Client computers.

- Denies write access to files and folders to help prevent viruses from modifying files
- Assesses computers on your network for vulnerabilities that make it prone to the current outbreak
- Deploys the latest components such as the virus pattern file and virus cleanup engine
- Performs a **Cleanup** on all the computers affected by the outbreak
- If enabled, scans your computers and networks and takes action against detected threats

See also: For information about setting ports to exclude from blocking, refer to the Client Server Security *Administrator's Guide*.

Current Status

The Security Dashboard displays and tracks the status of a world-wide virus outbreak threat on the Current Status screen. The status roughly corresponds to the outbreak life cycle.

During an outbreak threat, Outbreak Defense uses a three-stage strategy to protect your computers and networks. In each stage, it refreshes the information in the Current Status page.

The three stages of Outbreak Defense:

- Threat Prevention
- Threat Protection
- Threat Cleanup

FIGURE 4-3. Outbreak Defense Screen – Displaying No Current 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

Prevention

Threat Information					
Threat	Alert Type	Risk Level	Delivery Method	Vulnerability Exploited	Automatic Response
N/A					<input type="button" value="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 4-4. Outbreak Defense Screen – Prevention Stage

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 16:47:35 Refresh

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	MS08-036	<input type="button" value="Disable"/>
Date/Time Initiated		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 ID MS08-036 (modified, for testing). Need TMVAINFO.xml to create a fake to support and using special tsc.exe, tsc.ptn					

Threat Information

The Threat Information section displays information about viruses that are currently on the Internet and that could potentially affect your computers and network.

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

This panel displays a total number of Client computers that do and do not have automatic alert enabled. If alerts are not enabled, the Client computers cannot be notified to download components, run scans, and perform Cleanup.

Vulnerable Computers

This panel displays the names of the computers on your network that are vulnerable to the current threat. Click on a computer to view detailed information about the threat and the available patches to repair the vulnerabilities that the threat exploits.

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 4-5. 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	3.260.0000	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 status of the Client computers components
Click the numbered links for a list of specific computers.

Threat Cleanup

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

FIGURE 4-6. 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) Page: 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

- **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

Note: You can enable Outbreak Defense to send a notification to the Client/Server Security Agents to run a scan immediately after downloading the latest components during an outbreak from the **Outbreak Defense > Settings** screen.

Potential Threat

The Potential Threat screen displays information about security risks to your computers and network. The Security Server gathers threat information by running Vulnerability Assessment and Cleanup services.

Unlike the Current Threat screen that only displays information about a current threat, the Potential Threat screen displays information about all the threats to your computers and network that have not been resolved.

Vulnerable Computers

The Vulnerable Computers panel lists all the computers on your network that have vulnerabilities discovered since the last vulnerability assessment. You can view the Last updated time in the top-right hand corner of the screen.

The Potential Threat screen ranks the computers according to the risk level that they pose to the network. Risk level is calculated by Trend Micro and represents the relative number and severity of vulnerabilities for each computer.

When you click **Scan for Vulnerabilities Now**, Client Server Security runs a Vulnerability Assessment. A Vulnerability Assessment checks all the computers on your network for vulnerabilities and displays the results in the Potential Threat screen. Vulnerability Assessments can provide the following information about computers on your network:

- Identify vulnerabilities according to standard naming conventions
Find out more about the vulnerability and how to resolve it, by clicking on the vulnerability name.
- Display the vulnerabilities by computer and IP address
Results include the risk level that the vulnerabilities represent to the computer and to the entire network.
- Report vulnerabilities
Report vulnerabilities according to individual computers and describe the security risks those computers present to the overall network.

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.

Computers to Cleanup

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

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

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

To accomplish these tasks, Cleanup makes use of these components:

- Virus cleanup engine – the engine Cleanup uses to scan for and remove Trojans and Trojan processes
- Virus cleanup pattern – used by the virus cleanup engine
This template helps identify Trojan files and processes so the virus cleanup engine can eliminate them.

Cleanup runs on the Client computer on these occasions:

- Client users perform a manual cleanup from the client console
- You perform Cleanup Now on the client from the Trend Micro Security Dashboard for SMB
- Client users run a manual Scan or Clean
- After hot fix or patch deployment
- When the Security Server restarts

Because Cleanup 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, the Security Server may sometimes notify the user to restart their computer to complete the process of removing a Trojan or other malware application.

Setting Up Outbreak Defense

Client Server Security initiates Outbreak Defense in response to instructions that it receives in the Outbreak Prevention Policy. The Trend Micro Outbreak Prevention Policy is designed and issued by TrendLabs to give optimal protection to your computers and network during outbreak conditions. TrendLabs issues the Outbreak Prevention Policy when it observes frequent and severe virus and other malware incidents that are actively circulating on the Internet.

By default, the Security Server downloads the Outbreak Prevention Policy from the Trend Micro ActiveUpdate server every 30 minutes or whenever the Security Server starts up.

During Outbreak Defense, the Security Server enacts the Outbreak Defense Policy and takes action to protect your computers and network. At such a time, the normal functions of your network will be interrupted by such measures as blocked ports and inaccessible directories. You can use the Outbreak Defense Settings to customize the Outbreak Defense for your computers and network, thus avoiding unexpected consequences from the policies enacted during Outbreak Defense.

Note: Trend Micro designed Outbreak Defense defaults to provide optimal protection for your computers and network. Before customizing your Outbreak Defense settings, carefully consider the settings and only modify them when you understand the consequences.

Trend Micro recommended settings

- Enable Outbreak Defense for Red Alerts issued by Trend Micro
Outbreak Defense policies stay in effect until you click **Outbreak Defense > Current Threat > Disable** or one of the disable settings are met. When the Security Server downloads a new Outbreak Prevention Policy, the old policy stops.
- Disable Red Alerts after 2 days—define the duration for the Outbreak Defense.
- **Disable Red Alerts after required component(s) deployed:** when a Client computer downloads the required component, the Outbreak Defense policies no longer apply to that computer.

- **Exclusions:** the following ports will not be blocked during Outbreak Defense Automatic Response.
 - DNS
 - NetBios
 - HTTPS
 - HTTP (Web server)
 - Telnet
 - SMTP (Simple mail protocol)
 - FTP (File transfer protocol)
 - Internet Mail (POP3)
- **Scheduled Policy Download Settings:** the Security Server checks for new Outbreak Prevention Policies every 30 minutes and downloads new policies as required.
 - Download every 30 minutes
 - Source: Trend Micro ActiveUpdate server

Working with Security Settings

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

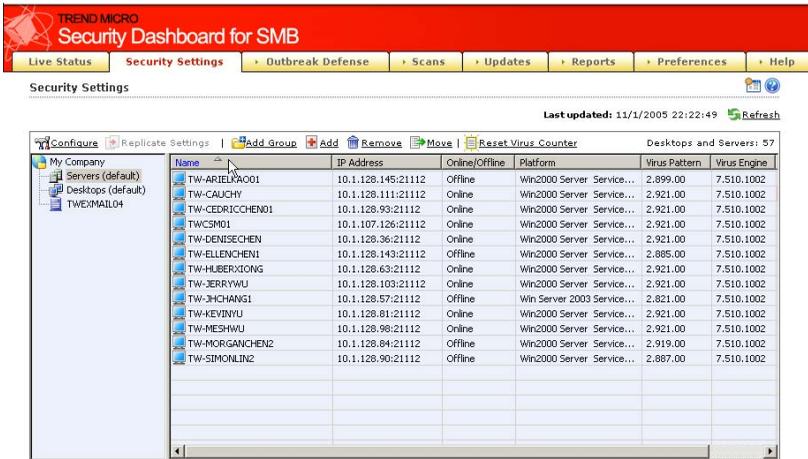
You can organize the computers where you have installed Client/Server Security Agents into groups. A group in Client Server Security is a group of Client computers that share the same security settings and run the same tasks. By grouping your Client computers, you can simultaneously configure, manage, and apply the same configuration to all group members.

Tip: For ease of management, group Client computers based on the departments to which they belong or the functions they perform. Also group Client computers that are at a greater risk of infection and apply a more secure configuration to all of them in just one setting.

When you select a computers from the left side and click **Configure**, the Security Dashboard displays a new configurations area, but the Security Dashboard menu items remain accessible.

Viewing the Security Settings Screen

The Security Settings screen displays all the Client computers that are protected by the Client/Server Security Agents.

FIGURE 4-7. The Security Settings Screen Showing Client Computers

After a Fresh Install

If you have installed Client Server Security for the first time, you will see two default computer groups in this screen: Servers and Desktops. Client Server Security automatically adds the computers and servers it detects on your network to these groups.

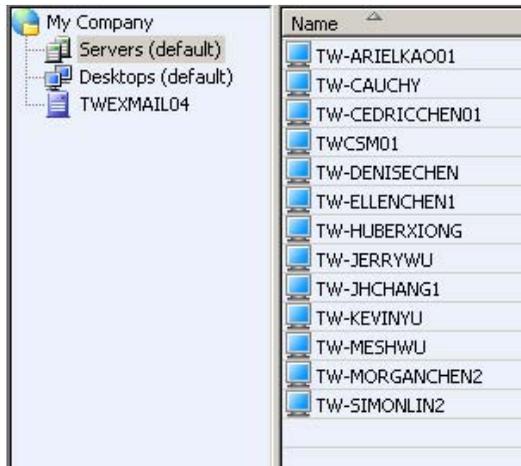
After an upgrade

If you have upgraded Client Server Security from a previous or trial version, Client Server Security preserves your old computers and groups in the Security Groups Tree.

Client Server Security 3.6 does not support individual settings within a group. If your prior version contained these, they will now appear as a "mixed" group.

Viewing the Client Server Security Security Groups Tree

The Security Groups Tree displays all the groups and Client computers connected to your network.

FIGURE 4-8. The Client Server Security Groups Tree

The Security Groups Tree

Client computers are displayed according to their group in the Security Groups Tree. The Security Groups Tree is an expandable list of logical groups of Client computers. When you select a group from the Security Groups Tree on the left side, a list of the computers in the group appears to the right. Select individual computers from the list on which to perform **Move** or **Remove** tasks.

Tip: To select multiple, adjacent Client computers, click the first computer in the range, hold down the SHIFT key, and then click the last computer in the range. To select a range of non-contiguous Client computers, click the first computer in the range. Hold down the CTRL key and then click the computer that you want to select.

Viewing the Security Settings Toolbar

The Security Settings Toolbar contains the tools you need to work with Client Server Security Groups and Client computers.

FIGURE 4-9. The Security Settings Toolbar



Using the Toolbar

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

TABLE 4-4. Tools for Security Settings

Tool	Description
Configure	Configure desktop and server settings at a group level for such settings as scanning, personal firewall, desktop privileges, and quarantine directory.
Replicate Settings	Use this tool to replicate configuration settings from one group of Client computers to one or more other groups of Client computers.
Add Group	Use this tool to create a new group of Client computers.

Add	Use Add to install Client/Server Security Agents to Client computers. After adding a new Client computer, drag and drop the icon for that computer to a group of your choice.
Remove	Use this tool to either remove a Client computer or group icon from the Security Dashboard or uninstall the Client/Server Security Agent from the selected Client computer.
Move	Use this tool to move a Client computer from one Security Server to another Security Server.

Using Add to Deploy the Security Agents

Use the Add tool to install the Client/Server Security Agent program on desktops and servers.

To add the Client/Server Security Agent to desktops and servers:

1. On the main menu, click **Security Settings** to view the Security Settings screen.
2. Click the **Add** tool from the toolbar. The **Add Computer** screen appears.
3. Select the computer type and method of deployment.
 - **Desktop or server** – select this option to deploy the Client/Server Security Agent to a desktop or server
 - **Method** – select a method of deployment for the Client/Server Security Agent
 - Email notification install – select this to send an email with a link to install the Client/Server Security Agent program
 - Remote install – select this to deploy the Client/Server Security Agent remotely from the Security Server
 - Create domain login script – select this to deploy the Client/Server Security Agent using a domain login script
4. Click **Next**.

See also: For more information about installing Security Agents, refer to the *Administrator's Guide*.

Removing the Client/Server Security Agent from Desktops and Servers

Remove the Client/Server Security Agent from Client computers on the network using the Security Dashboard.

To remove the Client/Server Security Agent using the Security Dashboard:

1. On the Security Dashboard main menu, click **Security Settings**. The **Security Settings** screen appears.
2. Select the Client Computers from which the Security Agent is to be removed.
3. Click the **Remove** tool from the toolbar. The Remove computer screen appears displaying the following options:
 - **Remove the selected inactive agent(s)** – select to remove the icon for the Client/Server Security Agent from the Security Settings screen
 - **Uninstall the selected agent(s)** – select to completely uninstall the Client/Server Security Agent program from the Client computer and remove the icon from the Security Settings screen
4. Click **Apply**.
5. Click **OK** when prompted to verify your decision to remove the Client/Server Security Agent.

Note: Selecting **Remove the selected inactive agent(s)** from the **Remove Computer** screen only removes the icon from the Security Settings screen, but the Client/Server Security Agent remains installed on the Client computer. Clicking **Uninstall the selected agent(s)** removes the Security Agent program running on the Client computer.

Configuring Security Tasks

This chapter tells you how to get up and running with Client Server Security. It includes topics such as:

The topics discussed in this chapter include:

- *Understanding the Threats* starting on page 5-2
- *Setting Real-time Antivirus Options for Desktops and Servers* starting on page 5-4
- *Granting Desktop Privileges* starting on page 5-5

Understanding the Threats

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

Malware

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 its type, may or may not include replicating and non replicating malicious code.

Client/Server Security Agents can detect malware during Real-time scanning or Manual and Scheduled scans.

Viruses

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

In addition to replication, some computer 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.

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

Network Viruses

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

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

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.

Client/Server Security Agents can detect Trojans during Antivirus scanning. Trojans do not infect files, thus cleaning is not necessary. The Trend Micro recommended action for Trojans is *delete*. To remove a Trojan, run **Cleanup**.

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

People use Packer tools to compressed Windows or Linux executable program. Compressing an executable makes the code contained in the executable more difficult for traditional Antivirus scanning products to detect. A Packer can conceal a Trojan or worm. The Trend Micro scan engine can detect Packer files and the recommended action for Packer files is *quarantine*.

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.

Client/Server Security Agents can detect worms during Antivirus scanning. Worms cannot be cleaned because they are self-contained programs. The Trend Micro recommended action for worms is *delete*.

Setting Up and Running Security Tasks

From the Security Settings screen you can set the Client/Server Security Agents to run security tasks on your Client computers. Trend Micro provides default settings for these tasks that are designed to give optimal protection for small and medium-sized businesses. This guide gives a description of the key tasks. For a more detailed information about how to customize these tasks, refer to your *Client Server Security 3.6 online help*.

By default, Real-time Antivirus is enabled and the Personal Firewall is disabled.

To set a task or configuration for a computer or group of computers:

1. Select the computer or groups of computers from the Group Management Tree.
2. Click **Configure**. A new menu appears on the left-hand side of the screen allowing you to set the tasks and configuration options for your computer or group.
3. Click a configuration item from the sidebar menu on the left-hand side of the screen.

Setting Real-time Antivirus Options for Desktops and Servers

Real-time scanning is an ongoing scan that runs in the background. Whenever it detects a file containing a virus or other malware, it performs the user-configured action against that virus or malware and sends the information to the Security Server database to be included in the logs. When enabled, Client/Server Security Agents can display alert messages, showing the name of the infected file and the virus or malware name, when it detects a virus or other malware on a Client computer.

The speed of Real-time scanning depends on your settings. You can increase the performance of real-time scans by decreasing the amount of files for scanning or by limiting the maximum number of compression layers to scan.

Trend Micro recommended default settings

- Real-time scanning is enabled and scans all incoming and outgoing files on your Client computers

- Files scanned—IntelliScan uses Trend Micro recommended settings to optimize scanning speed
- Action on detected threats—*clean* all detected files or *deletes* files that cannot be cleaned
- Advanced scanning options—scan all compressed files up to two compression layers deep
- Exclusions—excludes scanning folders where other Trend Micro products are installed

Setting Firewall Options for Desktops and Servers

Client Server Security includes a Personal Firewall to screen some types of communications with the Internet. By default, the Personal Firewall is disabled. If you enable the Personal Firewall, Trend Micro recommends the **Simple mode** for small and medium-sized businesses.

To customize your Firewall configuration, select **Advanced mode**. The Advanced mode is set to initially use the Trend Micro default configurations for **Simple mode**.

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.

Granting Desktop Privileges

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

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

Setting Up the Quarantine Folder for Desktops and Servers

When the Client/Server Security Agent detects files containing viruses or other malware, it quarantines the detected files to a folder on the Client computers. From this folder, the quarantined files are redirected to the Quarantine folder on the Security Server.

The default location of the Security Server quarantine folder is as follows:

```
Security Server\PCCSRV\Virus
```

The default directory on the Client computers is:

```
Client Server Security Agent/SUSPECT
```

Define the location of the Quarantine folder on the Security Server by typing a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path in the Quarantine Directory screen.

Managing Reports

Generate One-time Reports to view log information in an organized and graphically appealing format. You can print reports or send them by email to an administrator or other specified address.

FIGURE 5-1. Create One-time Report Screen



Generating Reports

Use one of the following methods to generate reports:

- Manually generate One-time reports
- Set a schedule to have the Security Server generate reports for you
Scheduled reports follow templates. To generate scheduled reports, first set up a template and then set the schedule for the template. The Security Server generates an individual report based on the template each time the schedule runs.

Deleting Reports

Reports can accumulate quickly if not deleted. Deleting reports can be a time-consuming and tedious task. Client Server Security allows you to automate this task.

Note: Reports are based on logs. When the log information is deleted, reports can no longer be generated.

Setting Global Preferences

Click **Preferences > Global** settings to open the corresponding screen. You can use the Global Preferences screen to set up the proxy server and SMTP server. You can also use it to configure System and Desktop/Server settings that apply to all the computers protected by Client Server Security.

Trend Micro provides default settings for your Global Preferences. If you want to customize your settings, refer to the *Client Server Security 3.6 online help*.

Contacting Support

This chapter tells you how to solve common problems and how to contact technical support. This chapter includes the following topics:

- *Contacting Trend Micro* starting on page 6-2
- *Contacting Technical Support* starting on page 6-2

Contacting Trend Micro

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

<http://www.trendmicro.com/en/about/contact/overview.htm>

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

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

Best Practices to Protect Your Computers and Network

There are many steps you can take to protect your computers and network from viruses and other types malware. Trend Micro recommends the following actions:

- Use the Trend Micro recommended Client Server Security default settings.
- Keep your Windows operating systems updated with the latest patches from Microsoft.
- Use strong passwords and advise your client users to use strong passwords. A strong password should be at least eight characters long and use a mixture of capital and lower case letters and numbers. It should never contain personal information about the user. Change your passwords every 60 to 90 days.
- Disable all unnecessary programs and services to reduce potential vulnerabilities.
- 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 that they can trust both the creator of the software they are downloading and the Web site source from where they are downloading the software).
 - Disregard unsolicited commercial email (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.
- Disallow the use of peer-to-peer file-sharing services. Viruses and other malware 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. If you find an application or file that Client Server Security cannot detect as a virus or other malware, 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

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

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

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.
Attachment	A file attached to (sent with) an email message.
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.

Term	Description
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 Security main program, the Security Server.
Client computers	The Client computers are all the desktops, laptops, and servers where the Client/Server Security Agents are installed. Client/Server Security Agents perform Antivirus scanning and Firewall configurations on Client desktops and 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.
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.
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. Lacking decryption codes, Client/Server Security Agents cannot scan encrypted files.

Term	Description
End User License Agreement (EULA)	<p>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.</p> <p>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.</p>
Exceptions	<p>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.</p>
File name extension	<p>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.</p>
File Transfer Protocol (FTP)	<p>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.</p>
File type	<p>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.</p>
Firewall	<p>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.</p>
FQDN (fully qualified domain name)	<p>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.</p>
FTP (file transfer protocol)	<p>FTP is a standard protocol used for transporting files from a server to a client over the Internet.</p>
Grayware	<p>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.</p>
Hot fixes and patches	<p>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.</p>

Term	Description
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.
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.
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 Client/Server Security Agent 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.

Term	Description
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 computer's 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 Client/Server Security Agents. End users can then set the Client/Server Security Agents to scan their Client computers according to the privileges you allowed. Use desktop privileges to enforce a uniform antivirus policy throughout your organization.
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.
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.

Term	Description
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 Client/Server 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 Security, you install it on a Windows server that becomes the Security Server. The Security Server communicates with the Client/Server Security Agents installed on Client computers. The Security Server also hosts the Security Dashboard, the centralized Web management console for the entire Client Server 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 Client/Server Security Agents.
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.
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.

Term	Description
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

- activating Client/Server Security 2-5
- Activation Code
 - required for installation 3-2
- ActiveUpdate
 - about 4-2
- Add
 - how to use 4-25
 - using to install Client/Server Security Agent 4-25
- Add Group
 - how to use 4-24
- administrator account
 - required for installation 3-3
- Administrator's Guide, how to use 2-3
- alerts
 - red alert 4-8
 - yellow alert 4-8
- Antivirus
 - components 1-5
- Antivirus scan results, displayed in Live Status 4-8
- automatic response
 - disabling 4-13
- automatic response details
 - viewing 4-13

B

- blocking ports, during Outbreak Defense 4-8, 4-11
- blocking shared folders, during Outbreak Defense 4-11

C

- cleanup
 - during Outbreak Defense 4-11
- cleanup stage, Outbreak Defense 4-10
 - explained 4-15
- Client computer groups
 - configuring 5-4
- Client Computers, described 1-3
- Client/Server Security
 - diagram, Figure 1-1 1-4
 - protection strategy 1-7
- Client/Server Security Agent
 - default actions 5-5

- deploying after installation 3-5
- desktop privileges, granting 5-5
- IntelliScan, default scanning method 5-5
- managing from Security Settings 4-21
- minimum system requirements 3-3
- part in protection strategy 1-7
- real-time Antivirus scans, default settings 5-4
- using Add to install 4-25

Client/Server Security Agent, described 1-3

components

- conditions for automatic updates 4-2
- downloaded during Outbreak Defense 4-8, 4-11

components, Client/Server Security 1-4

Configure

- how to use 4-24

configuring groups 5-4

contacting technical support 6-2

contacting Trend Micro 6-2

Custom installation

- overview 3-4

D

Dashboard password, required for installation 3-2

default settings

- Client/Server Security Agent, real-time Antivirus scans 5-4
- component download source 4-9
- notifications 4-6
- scheduled updates 4-2
- Security Settings 5-4

denied write access, during Outbreak Defense 4-11

deploying Client/Server Security Agent 3-5

desktop privileges

- granting 5-5

disabling

- automatic response 4-13

disabling alerts 4-19

documentation

- overview 2-3

domain administrator privileges

- required for installation 3-3

domain name, Security Server

- required for installation 3-2

E

email notification, installing the Client/Server Security Agent 4-25

enabling alerts 4-19
evaluation version
 upgrading 3-16
excluded ports, during Outbreak Defense 4-20
expired license, consequences 2-7

F

firewall, personal
 setting options 5-5

G

generating reports 5-7
Getting Started Guide, how to use 2-3
global preferences
 proxy server 5-7
 setting 5-7
 SMTP server 5-7
granting desktop privileges 5-5
Group Management Tree, described 4-24
groups
 configuring 5-4
 in Security Settings screen 4-21
 preserved during upgrade 4-22

H

help, using icon to access 4-5
hostname, Security Server
 required for installation 3-2

I

individual settings for Client computers, not supported 4-22
installation
 overview, stages 3-5
 performing Typical 3-5
installation methods
 Custom installation 3-4
 Silent installation 3-4
 Typical installation 3-4
installing Client/Server Security Agent 4-25
IntelliScan
 default scanning method for Client/Server Security Agent 5-5
IP address, Security Server
 required for installation 3-2

K

Knowledge Base, how to use 2-4

L

license

- benefits 2-6
- changing 2-5
- consequences of expiry 2-7
- information in Live Status 4-9

Live Status

- part in protection strategy 1-8
- viewing 4-6

logs

- deleting before upgrade 3-15
- stored on the Security Server 1-2

M

maintenance agreement 6-2

malware, defined 5-2

minimum system requirements

- Client/Server Security 3-3
- Client/Server Security Agent 3-3
- Security Server 3-3

mixed groups 4-22

Move

- how to use 4-25

N

Network Virus

- components 1-6

network virus scan results, displayed in Live Status screen 4-9

network viruses

- defined 5-2

Notifications

- part in protection strategy 1-8

notifications

- default settings 4-6
- setting up 4-5

O

official pattern release

- triggered by red alert 4-8

one-time reports

- managing 5-6
- manually generating 5-7

online help, how to use 2-3

Outbreak Defense

- blocking ports 4-11

- blocking shared folders 4-11
- cleanup 4-11
- cleanup stage 4-10
- components 1-6
- denying write access 4-11
- disabling alerts 4-19
- enabling alerts 4-19
- excluding ports from blocking 4-20
- part in protection strategy 1-8
- prevention stage 4-10
- protection stage 4-10
- scanning 4-11
- Security Server actions 4-19
- stages, table 4-3 4-10
- updating components 4-11
- vulnerability assessment 4-11
- outbreak life cycle 4-10
- Outbreak Prevention Policy 4-19
 - download frequency 4-20
 - download source 4-20

P

- Packer, defined 5-3
- password
 - required for Uninstall 3-3
 - required for Unload 3-3
- personal firewall
 - blocks network viruses 5-2
 - setting options 5-5
- prevention stage
 - explained 4-13
 - Outbreak Defense 4-10
- privileges, domain administrator
 - required for installation 3-3
- protection stage, Outbreak Defense 4-10
- proxy server, setting global preferences 5-7

Q

- quarantine folder
 - setting for desktops and servers 5-6
- quarantine folder, desktops and servers
 - default directory 5-6
- Quick Tour, using icon to launch 4-5

R

- real-time antivirus scans

- setting 5-4
- real-time scanning 5-4
 - speed of 5-4
- red alert
 - about 4-8
 - trigger conditions 4-8
 - trigger official pattern release 4-8
- refresh icon 4-5
- registering Client/Server Security 2-5
- Registration Key
 - required for installation 3-2
- Remove
 - how to use 4-25
- Replicate
 - how to use 4-24
- reports
 - deleting 5-7
 - one-time reports, managing 5-6
- reports, generating 5-7

S

- scans
 - during Outbreak Defense 4-11
- scans, during Outbreak Defense 4-8
- scheduled updates, Security Server
 - hourly, by default 4-2
- Security Dashboard
 - major features, overview 4-4
 - opening 4-3
- Security Dashboard, described 1-2
- Security Server
 - action during Outbreak Defense 4-19
 - component updates, hourly 4-2
 - minimum system requirements 3-3
 - part in protection strategy 1-7
- Security Server, described 1-2
- Silent installation
 - overview 3-4
- Simple Mail Transport Protocol (SMTP)
 - definition B-6
- SMTP server
 - global preferences 5-7
- SMTP server name, required for installation 3-2
- SOCKS 4
 - definition B-6

startup
 automatic update 4-2

T

technical support
 contacting 6-2

Telnet

 definition B-6

threat status, in Live Status 4-7

threat type

 malware 5-2

 network virus 5-2

 virus 5-2

threat types

 packer 5-3

 Trojan 5-3

 worm 5-3

Toolbar

 using 4-24

Transmission Control Protocol (TCP)

 definition B-6

Trend Micro

 contacting 6-2

TrendLabs 4-19

 definition B-6

Trojan horse program (Trojan), defined 5-3

Trojan horses

 definition B-6

Typical installation

 overview 3-4

 running 3-5

U

Uninstall

 requires password 3-3

Unload

 requires password 3-3

updates

 automatic 4-2

 information in Live Status 4-9

upgrade

 deleting log files before 3-15

 from evaluation version 3-16

 preserving client settings 3-15

upgrading

from previous version 3-15
supported upgrades 3-15

V

viruses, defined 5-2
vulnerability assessment, during Outbreak Defense 4-11

W

worms, defined 5-3

Y

yellow alert
about 4-8
trigger conditions 4-8